FÖRSVARSHÖGSKOLAN

LAG OCH ORDNING I CYBERRYMDEN – EN JÄMFÖRELSE AV FINLANDS OCH SVERIGES CYBERSSÄKERHETSPOLITIK MELLAN ÅREN 2009–2015, MED FOKUS PÅ LAGSTIFTNINGEN

Kandidatuppsats

Kadettundersergeant
Ted Rönnberg

82. sjökadettkursen
Sjöbevakningslinjen

Mars 2015

FÖRSVARSHÖGSKOLAN

Kurs	Linje
82. sjökadettkursen	Sjöbevakningslinjen

Skribent

Kadettundersergeant Ted Rönnberg

Studiens namn

LAG OCH ORDNING I CYBERRYMDEN – EN JÄMFÖRELSE AV FINLANDS OCH SVERIGES CYBERSSÄKERHETSPOLITIK MELLAN ÅREN 2009–2015, MED FOKUS PÅ LAGSTIFTNINGEN

Läroämne, som studien är kopplat till	Förvaringsplats
Strategi	Försvarshögskolans kursbibliotek
Tid Mars 2015	Textsidor 43 Sidantal på bilagor 1

SAMMANDRAG

Denna undersökning har jämfört Finlands och Sveriges cybersäkerhetspolitik. Som forskningsmetod har använts komparativ analys och som teoretisk referensram säkerhetiseringsteorier. Rubriken har valts på grund av den aktuella samhällsdebatt som förs kring cyberssäkerhet. Statliga dokument har använts som primära källor. Intervjuer, artiklar och nyheter har använts för att stöda slutsatserna. Lagstiftningen har lagts i fokus, eftersom den styr själva verkställandet av idkad cybersäkerhetspolitik.

Utförd analys visar att Finland och Sverige behandlar cybersäkerhetsfrågorna som en del av den övriga säkerhetspolitiken. Den största skillnaden är att Sverige inte har ett lika synligt behov att säkerhetisera sin cybersäkerhetsagenda. Detta beror på att Sverige redan säkrat sina statliga säkerhetsintressen i cyberrymden tack vare den så kallade FRA-lagen. Analysen visar att Finland med sin säkerhetisering strävar efter likande befogenheter åt myndigheterna att bedriva underrättelse i cyberrymden. Målet för Sveriges säkerhetisering är enligt denna analys att stärka de existerande säkerhetsstrukturerna och utveckla myndighetssamarbete.

Lagstiftningsanalysen visar att båda länderna betonar medorgarnas grundläggande friheter och rättigheter, yttrandefrihet samt personlig integritet på nätet. En annan likhet är att båda strävar att lösa lagstiftningsfrågorna genom internationellt samarbete. Den största skillnaden mellan Finland och Sverige är att Sverige endast försöker anpassa den nuvarande lagstiftningen till cyberdomänen, medan Finland strävar att forma en helt ny cyberlagstiftning. Slutsatsen visar dock att staterna först måste definiera cyberterminologin juridiskt, innan de kan göra straffrättsliga tolkningar. Därtill måste länderna utveckla regelverken för överlåtelse av information myndigheterna emellan.

NYCKELORD
cybersäkerhet, informationssäkerhet, säkerhetspolitik, cybersäkerhetsstrategi, säkerhetisering

LAG OCH ORDNING I CYBERRYMDEN – EN JÄMFÖRELSE AV FINLANDS OCH SVERIGES CYBERSSÄKERHETSPOLITIK MELLAN ÅREN 2009–2015, MED FOKUS PÅ LAGSTIFTNINGEN

INNEHÅLL

CENTRALA FÖRKORTNINGAR OCH BEGREPP

Denna lista redogör för en del centrala förkortningar och begrepp som förekommer i denna undersökning. För begrepp som saknar entydiga vetenskapliga definitioner presenteras de medvetna tolkningar som denna undersökning gör.

Aktiv nätspaning	Utförandet av övervakning och underrättelse av datatrafik utanför egna undernätverk i cyberrymden.
CCD CoE	Co-operative Cyber Defence Center of Exellence. NATOs cyberförsvarscenter.
Cyber-	Termen används i sammansatta ord i anknytning till digital informationsteknik, dataöverföring, datasystem och elektroniska informationssystem.[1]
Cyberdomän eller *cybersäkerhetsdomän* (substantiv, *-en -er*)	Det säkerhetsområde som cybersäkerheten utgör. Inom militärsäkerhet anses cyberdomänen vara en domän vid sidan om land-, luft-, hav- och rymddomänerna.
Cyberrymd	Den virtuella dimensionen som kopplar ihop digitala nätverk. Internet utgör det största enskilda delområde i cyberrymden.
Cybersäkerhet	Tryggandet av cyberomgivningens funktioner. Detta innebär funktionssäkerhet, störningsfrihet och skydd av elektronisk information, mot fientlig verksamhet.[2]
Cybersäkerhetspolitik	Statsmaktens åtgärder för att förbättra den nationella cybersäkerheten.
EU	Europeiska Unionen (Europeiska unionen).
FN	Förenta nationerna. En global fredsorganisation.
FRA	Försvarets radioanstalt; en civil underrättelsemyndighet i Sverige, vars uppgift är att stöda Sveriges utrikes-, säkerhets- och försvarspolitik.[3]
FRA-lagen	Namnet syftar på *Lag* (2008:717) *om signalspaning i förunderrättelseverksamhet*. I korthet ger lagen Försvarets radioanstalt rätten att med domstolsbeslut utföra signalspaning på all kabelburen trafik, som passerar Sveriges gränser.[4]

[1] Finlands försvarsministerium. *Strategi för Cybersäkerheten i Finland*. Statsrådets principbeslut 24.1.2013, Helsingfors 2013, s.12.
[2] International Telecommunication Union (ITU), webblpats. [http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx / 24.3.2015]
[3] Försvarets radioanstalt (FRA), *Om FRA*. [http://www.fra.se/omfra.6.html / 25.3.2015]
[4] Sveriges försvarsdepartement, *Lag om signalspaning i försvarsunderrättelseverksamhet*, lag (2008:717), Stockholm 2008.

Försörjningsberedskapscentarlen	Ett sammarbetsorgan mellan myndigheter och centrala ekonomiska aktörer i samhället. Centralens uppgift är att upprätthålla samhällets ekonomiska basfunktioner.
Handlingsregler	Instruktioner och modeller hur myndigheterna bör agera i olika situationer.
HAVARO	Systemet för upptäckandet av kränkningar mot informationssystemen. HAVARO administreras av Kommunikationsverket.
Informationssäkerhet	Arrangemang för att trygga att datasystemen är fungerande och att informationen är användbar och konfidentiell[5]. Sverige har dessutom valt att behandla cybersäkerhetsfrågor under begreppet informationssäkerhet.
KPMG	Ett internationellt revisions- och rådgivningsföretag.
Lägesbild	Medvetenhet om händelser inom en godtycklig omgivning.
MSB	Myndigheten för samhällsskydd och beredskap. Myndigheten för samhällsskydd och beredskap är en civil myndighet i Sverige vars uppgift är att förebygga och hantera olyckor och kriser.[6]
NATO	North Atlantic Treaty Organization (Nordatlantiska fördragsorganisationen). En militär allians.
OECD	Organisation for Economic Co-operation and Development. Organisationens främsta uppgift är att arbeta för en fungerande marknadsekonomi och social välfärd, mellan de demokratiskt styrda medlemsländerna.[7]
Passiv nätspaning	Utförandet av övervakning och underrättelse av datatrafik inom egna undernätverk.
Signalspaning	Inhämtning av informationsbärande signaler och data och analysera dem. Signalspaning kan utföras på radiosignaler eller kabelburen trafik.[8]
Säkerhetisering	En metod för att driva säkerhetspolitik, som baserar sig på konstruktivistiska säkerhetsteorier.[9]
Säkerhetskommittén	En kommitté som bistår statsrådet och ministerierna i breda säkerhetsfrågor.
Säkerhetsstruktur	De strukturer och funktioner som utgör grunden för upprätthållandet av samhällsordning.

[5] Finlands försvarsministerium (2013) *Strategi för Cybersäkerheten i Finland*.
[6] Myndigheten för samhällsskydd och beredskap (MSB), webbplats. [https://www.msb.se / 24.2.2015]
[7] OECDs, webbplats. [http://www.oecd.org/about/ / 24.3.2015]
[8] Försvarets radioanstalt (FRA), *Signalunderrättelseverksamhet*.
[http://www.fra.se/verksamhet/signalunderrattelseverksamhet.68.html / 25.3.2015]
[9] Buzan, Barry & Wæver, Ole & de Wilde, Jaap. *Security: A New Framework for Analysis*, Lynne Rienner Publishers, London 1998.

LAG OCH ORDNING I CYBERRYMDEN – EN JÄMFÖRELSE AV FINLANDS OCH SVERIGES CYBERSSÄKERHETSPOLITIK MELLAN ÅREN 2009–2015, MED FOKUS PÅ LAGSTIFTNINGEN

1 INLEDNING

Cyberdomänen har vuxit exponentiellt under det senaste decenniet, vilket har lett till nya politiska utmaningar som bland annat är säkerhets- och samhällspolitiska, samt ekonomiska och militära. År 2013 utgav Finland sin första officiella cybersäkerhetsstrategi[10]. Senare samma år, framkom det att Utrikesministeriet hade blivit utsatt för dataintrång utan att vara medveten om det[11]. Nätverksspionaget hade pågått i ca fyra år[12]. Enligt uppgifter från Sveriges Radio, avslöjades spionaget av Försvarets radioanstalt (FRA)[13]. Dataintrånget visade att Finland hade misslyckats i att skydda sina statshemligheter mot cyberattacker, trots att Finland hade gjort den digitala informationssäkerheten till en säkerhetspolitisk prioritet redan fyra år tidigare i *Statsrådets säkerhets- och försvarspolitiska redogörelse* 2009[14].

Denna undersökning jämför Finlands och Sveriges cybersäkerhetspolitik med hjälp av *komparativ analys*[15], som forskningsmetod och *säkerhetisering*[16] som teoretisk referensram. Därefter försöker undersökningen föreslå åtgärder som kunde förbättra Finlands cybersäkerhet. Därmed kommer arbetet att ha en *normativ disposition*[17].

Lagstiftningsperspektivet har tagits i fokus, eftersom lagstiftningen starkt påverkar själva verkställandet av cybersäkerhetspolitiken. Lagstiftningen är aktuell särskilt därför att Finland

---

[10] Finlands försvarsministerium, *Strategi för cybersäkerheten i Finland*, [http://www.defmin.fi/sv/publikationer/strategidokument/strategi_for_cybersakerheten_i_finland / 18.4.2014]

[11] Finlands utrikesministerium, *Finlands utrikesförvaltning utsatt för dataintrång*, 1.11.2013. [http://formin.finland.fi/public/default.aspx?contentid=291720&nodeid=23&contentlan=3&culture=sv-FI / / 15.4.2014]

[12] MTV-uutiset 31.10.2013, *Suomen ulkoministeriö laajan verkkovakoilun kohteena*. [http://www.mtv.fi/uutiset/kotimaa/artikkeli/mtv3--suomen-ulkoministerio-laajan-verkkovakoilun-kohteena-vuosia/2369718 / 15.4.2014]

[13] Sveriges radio 3.11.2013, *Sverige avslöjade spionage i Finland*. [http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5693167 / 15.4.2014]

[14] *Finlands säkerhets- och försvarspolitik 2009*. Statsrådets redogörelse till riksdagen 5.2.2009, SRR 1/2009 rd, Helsingfors 2009.

[15] För närmare beskrivning se: Ragin, Charles C. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*, University of California Press Ltd, London 1989.

[16] Säkerhetisering syftar på eng. "securitization". Se: Buzan, B. & Wæver, O. & de Wilde, J. (1998) *Security: A New Framework for Analysis*.

[17] Sipilä, Joonas & Koivula, Tommi. *Kuinka strategiaa tutkitaan*, Maanpuolustuskorkeakoulu, Strategian laitos, julkaisusarja 2, Tutkimusselosteita No. 50, Helsingfors 2013, s. 38.

som bäst förbereder en lagförändring för övervakning, brott och bestraffning inom området för den digitala dimensionen[18]. Genom förändringen försöker Finland möta de behov som fastställts i den nationella cybersäkerhetsstrategin[19].

1.1 Syfte

Forskningens syfte är att jämföra Finlands och Sveriges cybersäkerhetspolitik och den rådande synen på cyberlagstiftningen.

1.2 Avgränsningar

Arbetet kommer huvudsakligen att betrakta den säkerhetspolitiska aspekten av cyberfrågor, genom analys av nationella säkerhetspolitiska dokument. För Finland är det centralaste dokumentet den nationella cybersäkerhetsstrategin som heter *Strategi för cybersäkerheten i Finland*.[20] Sverige har inte någon officiell cybersäkerhetsstrategi och därför måste Sveriges cybersäkerhetspolitik huvudsakligen analyseras utgående från övriga statliga dokument, relaterade till ämnesområdet. Johan Sigholm, doktor i militärteknik från Sveriges Försvarshögskola, berättar att Sverige inte har någon renodlad cybersäkerhetsstrategi. Myndigheten för samhällsskydd och beredskap (MSB) ansvarar för den civila cybersäkerheten och de har gett ut ett dokument som heter *Strategi för samhällets informationssäkerhet 2010–2015*[21]. Sigholm berättar att denna strategi som bäst genomgår en revidering. Han säger att tanken då är att knyta ihop allt flera samhällsområden i samma strategi. Sigholm berättar att Sverige ännu inte har militärt tagit ställning till cybersäkerheten, men att de kommer att göra det i sin *Militärstrategiska doktrin* år 2015.[22]

Undersökningen baserar sig på dokument från årsskiftet 2008–2009 till mars 2015. Tidsperioden är vald på grund av att 2009 är det år då Finland för första gången gjorde cybersäkerheten till en nationell prioriet i *Statsrådets säkerhets- och försvarspolitiska redogörelse*. Finland och Sverige har också under denna tid utgivit de statliga dokument som kraftigast styr

[18] YLE nyheter 3.7.2014, *Viranomaisia ei kiinnosta, mitä Facebookissasi tapahtuu*. [http://yle.fi/uutiset/haglund_viranomaisia_ei_kiinnosta_mita_facebookissasi_tapahtuu/7336651 / 4.7.2014]
[19] Finlands försvarsministerium (2013) *Strategi för Cybersäkerheten i Finland*.
[20] Catharina Candolin. Intervju 7.2.2014.
[21] Myndigheten för samhällsskydd och beredskap. *Strategi för samhällets informationssäkerhet 2010-2015*, Stockholm 2010.
[22] Sigholm, Johan. Brevväxling 15.2.2015.

cybersäkerhetspolitiken idag. Intervjuer och artiklar användas i andra hand, för att stöda utförd analys och i strävan att ge svar på öppna frågor.

Undersökningen kommer endast att behandla cybersäkerhetens strategiska aspekter. Den operativa och tekniska nivån kommer inte att granskas. Historiska händelser kommer endast att nämnas, såvitt de utgör något specifikt exempel.

Som teoretisk referensram använder sig arbetet av säkerhetiseringsteorier. Säkerhetiseringsteorierna är speciellt lämpliga därför att undersökningen analyserar ett icke-traditionellt säkerhetspolitiskt samhällsområde och därför att länderna är relativt små på den globala politiska spelplanen. Arbetet kommer inte att analysera hur Finland eller Sverige har lyckats säkerhetisera sin cybersäkerhetsagenda. Fokus kommer däremot att ligga på analys av tecken som påvisar att säkerhetisering har skett eller sker som bäst.

1.3 Metod

OECDs cybersäkerhetsrapport visat att komparativ analys är en fungerande forskningsmetod, då syftet är att jämföra cybersäkerhetsstrategier[23]. Därför har denna studie också valt komparativ analys som forskningsmetod. Enligt professor Pentti Luoma lämpar sig komparativ analys för undersökningar som påminner om fallstudier[24]. I en komparativ analys betraktas observationsenheterna som helheter, ur ett realförhållandeperspektiv. Observationsenheter kan till exempel vara länder, områden eller olika händelser.[25]

Forskningsansatsen kan antingen vara *variabelbaserad*[26] eller *observationsbaserad*[27]. Variabelbaserad betyder i praktiken att undersökningen i början väljer ut ett antal parametrar från jämförbara dokument som sedan analyseras sida vid sida.[28] Detta möjliggör statistiskanalys, genom vilket det går att påvisa trender. Vidare kan detta användas för att göra sannolikhetstolkningar.[29] I den observationsbaserade forskningsansatsen jämförs observationsenheterna

[23] OECD, "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, 2012. [http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf / 1.3.2014]
[24] Luoma, Pentti. *Johdatus kvalitatiiviseen vertailevaan analyysiin*, Oulun yliopisto 23.11.2006. [www.oulu.fi/sosiologia/node/5047 / 30.1.2015]
[25] Ibid.
[26] Ragin, C. (1989), s. 34–69.
[27] Ibid.
[28] Ibid.
[29] Luoma, P. [www.oulu.fi/sosiologia/node/5047 / 30.1.2015]

genom mera djupgående analys av observerade fenomen. Vanligtvis utväljs då bara en handfull med observationer.[30]

Eftersom Sverige inte har någon officiell cybersäkerhetsstrategi är det svårt att välja ut parametrar i förväg. Därför har denna undersökning valt den observationsbaserade forskningsansatsen, eftersom den möjliggör analyserandet av idkad cybersäkerhetspolitik på basis av godtyckliga, statliga, dokument. Ett kriterium är dock att dokumentens innehåll, på ett eller annat sätt, är relaterade till cybersäkerhet.

Nackdelen är att metoden inte klarar av att beakta många sakförhållanden och kännetecken samtidigt[31]. En annan nackdel är att denna metod inte tar i beaktande de historiska händelser som har lett till de observerade fenomenen[32]. Emellertid utgör detta inte något problem för denna studie, eftersom målet för denna undersökning är att jämföra de mest centrala helheterna i Finlands och Sveriges cybersäkerhetspolitik och dra slutsatser på basis av dessa.

1.4 Kontribution

Forskingen är en del av den säkerhetspolitiska forskning som görs vid Finlands Försvarshögskola och den är gjord på grund av ämnets aktualitet. Forskningen är aktuell fördenskull att ingen tidigare har jämfört Finlands och Sveriges cybersäkerhetspolitik. Detta beror högst antagligen på att Sverige inte ännu har någon officiell cybersäkerhetsstrategi. Sverige har valts som jämförelse land, på grund av Finlands och Sveriges närstående politiska relationer, samt på grund av den gemensamma syn som länderna har på myndigheternas roll i samhället.[33] En annan orsak till att Sverige har valts som jämförelse objekt är forskarens språkkunskaper i svenska.

Målet för denna analys är att stöda uppdaterandet av Finlands cybersäkerhetsstrategi i framtiden och att bidra till den allmänna diskussionen kring cybersäkerhetsfrågor. Det andra målet är att komma med konkreta förslag på hur Finland kunde förbättra sin lagstiftning, för att nå de strategiska målsättningarna. På så sätt har undersökning potential att stöda det kommande lagstiftningsarbetet i Finland. Undersökning kan möjligen också stöda ett eventuellt framtida

[30] Ragin, C. (1989), s. 34–69.
[31] Luoma, P. [www.oulu.fi/sosiologia/node/5047 / 30.1.2015]
[32] Ragin, C. (1989), s. 34–69.
[33] Nordiska ministerrådet, webbplats. [http://www.norden.org/sv/fakta-om-norden/politik / 24.3.2015]

cybersäkerhetssamarbete mellan Finland och Sverige, genom en ökad och ömsesidig förståelse för den andres cybersäkerhetspolitik.

1.5 Forskningsfrågor

0. På vilket sätt har Finland, respektive Sverige, valt att säkerhetisera sin cybersäkerhetspolitiska agenda?
0. Vilka är styrkorna och svagheterna i Finlands, respektive Sveriges, cybersäkerhetspolitik?
1. Hur anser länderna att lagstiftningen borde anpassas till cybersäkerheten?
2. Vilka åtgärder kräver implementerandet av Finlands cybersäkerhetsstrategi?

1.6 Arbetets upplägg

Kapitel två granskar huruvida säkerhetiseringsteorierna lämpar sig granskningen av cybersäkerhetsfrågor. Likaså övervägs teorins för- och nackdelar i kapitlet.

Det tredje kapitlet inleds med en kort sammanfattning av OECDs jämförelse av olika länders cybersäkerhetsstrategier. Kapitlet kommer därefter att analysera Finlands och Sveriges statliga dokument som behandlar cybersäkerhet. Den teoretiska referensramen kommer att appliceras vid utförandet av analysen. Arbetet kommer här att söka efter tecken som visar på vilket sätt respektive land har säkerhetisering sin cybersäkerhetspolitiska agenda. Med hjälp av denna genomgång av de statliga dokument kommer undersökningen att förbereda lagstiftningskapitlet, genom att förutspå resultat som eventuellt kan förväntas av lagstiftningsanalysen.

I det fjärde kapitlet kommer undersökningen att se på lagstiftningen som säkerhetspolitiskt verktyg. Samtidigt utgör detta en tvärvetenskaplig vinkling och en praktisk metod att behandla cybersäkerhetsfrågor. I detta kapitel diskuteras Försvarets radioanstalts juridiskt berättigade roll som säkerhetsmyndighet i cyberrymden och vad det har lett till i Sverige. Utifrån detta, försöker undersökningen konkludera vad Finland borde göra för att nå sina strategiska målsättningar.

Det femte kapitlet återger en kort genomgång av utförd analys och diskuterar vad detta innebär i framtiden. Implikationerna kommer främst att fokusera på Finland. Kapitel sex väger arbetets vetenskapliga värde och resultatens trovärdighet och det sista kapitlet sammanfattar undersökningens centrala slutsatser och resultat, som också är sammanställda till en tabell i bilaga 1.

2 SÄKERHETISERING SOM TEORETISK REFERENSRAM

Denna studie kommer inte att beskriva något djupgående vad säkerhetisering är, eftersom det redan finns förklarat i flera textböcker[34]. Undersökningen kommer däremot att se på hur säkerhetiseringsteorierna lämpar sig för granskningen av cybersäkerhetspolitik och vilka brister detta kan medföra.

Denna undersökning har valt säkerhetisering som teoretisk referensram, eftersom det är en fungerande metod för att analysera komplexa säkerhetsproblem, vilket cybersäkerheten i detta fall är. *Köpenhamnsskolan*[35] ger, enligt Ralf Emmers, en fungerande teori för en ”systematisk, komparativ och koherent” analys av säkerhetsfrågor. Med hjälp av den kan mångdimensionella säkerhetsfrågor analyseras, som samtidigt både är interna och externa.[36]

Jarno Limnéll, cybersäkerhetsprofessor vid Aalto-universitet och cybersäkerhetschef på McAfee, beskriver i sin doktorsavhandling att stater med hjälp av säkerhetisering definierar vad som hotar dem, för att på så sätt motivera sin närvaro i säkerhetsomgivningen[37]. Detta kan bland annat ske genom en *talesakt*[38], som i detta fall kan omfatta en officiell cybersäkerhetsstrategi och den övriga kommunikationen kring den[39].

Samitidigt som säkerhetiseringsteorierna har sina fördelar, medför det också utmaningar. Den största utmaningen för denna undersökning är att det inte finns någon entydig förklaring på vad säkerhet är[40] och att det därför inte heller existerar någon entydig definition på när något är säkerhetiserat[41].

För det andra har säkerhetiseringsteorierna den benägenheten att de inte explicit betonar den militära säkerheten, som kan tolkas som en av de högsta säkerhetsnivåerna i samhället[42]. Där-

---

[34] Se till exempel: Emmers, Ralf. “Securitization”, Collins, Alan. (ed), *Contemporary Security Studies*, 2nd ed., Oxford University Press, Oxford 2010.
eller
Bigo, Didier. “International Political Sociology”, Williams, Paul D. (ed), *Security Studies – An Intorduction*, 1st ed., Routledge, Abingdon 2008.
[35] Buzan, B. & Wæver, O. & de Wilde, J. (1998) *Security: A New Framework for Analysis*, s. 3–47.
[36] Emmers, R. (2010) “Securitization”, s. 137–149.
[37] Limnéll, Jarno. *Suomen uhkakuvapolitiikka 2000-luvun alussa*, Maanpuolustuskorkeakoulu, Strategian Laitos, julkaisusarja 1, Strategian tutkimuksia No. 29, Helsingfors 2009, s. 64–66.
[38] Talakt syftar på eng. ”speech act”. Talakt är det sätt på vilket man för fram sitt ärende i en säkerhetiseringsprocess. Se till exempel: Emmers, R. (2010) “Securitization”, s. 136.
[39] Paronen, Antti. Proseminarium 7.5.2014.
[40] Bigo, D. (2008) “International Political Sociology”, s. 118–123.
[41] Emmers, R. (2010) “Securitization”, s. 142.
[42] Paronen, A. Proseminarium 29.1.2015.

för är det sannolikt att de militärstrategiska aspekterna kommer att få en mindre roll i denna undersökning, gentemot om någon annan teoretisk referensram skulle tillämpas. Att de militära aspekterna inte beaktas kan få allvarliga konsekvenser om teorierna används för att dra militärstrategiska slutsatser. Denna problematik kvarstår emellertid, men minskar inte teoriernas användbarhet om de tillämpas på rätt sätt.

Den tredje nackdelen är att Köpenhamnsskolan har kritiserats för att vara ”Euro-centrisk”, eftersom den behandlar säkerhetsproblem ur ett Europeiskt perspektiv[43]. Detta kunde medföra diverse problem, ifall teorierna tillämpades på någon stormakt, eller om cybersäkerhetspolitiken skulle jämföras globalt. För denna studie utgör detta inte något problem, då analysen endast koncentrerar sig på en omgivning där den finska och svenska säkerhetspolitiken och säkerhetstänkandet står i centrum.

Slutligen kan det konstateras att teorierna inte kan ge svar på om säkerhetiseringen kommer att leda till en effektiv behandling av cybersäkerhetsärendet. De kommer inte heller att kunna förutspå om säkerhetiseringen kommer att leda till önskade slutresultat.[44]

2.1 Cybersäkerheten som säkerhetiseringssobjekt

Cyberdomänen är en mångdimensionell säkerhetsmiljö, som har uppstått på marknadsekonomins och den tekniska utvecklingens villkor[45]. Pekka Sivonen, professor i strategiska studier vid Finlands Försvarshögskola, säger att detta har lett till att cyberdomänen är en onaturlig säkerhetsmiljö för stater och att de därför explicit måste motivera sin närvaro som säkerhetsaktörer.[46] Säkerhetiseringsteorierna och Köpenhamnsskolan erbjuder i detta fall en alternativ referensram till de *traditionella*[47] säkerhetsteorierna. En av fördelarna är fördelen att säkerhetiseringsteorierna bättre beaktar icke-statliga aktörer.[48] Detta är en viktig aspekt då cybersäkerhet diskuteras.

[43] Emmers, R. (2010) “Securitization”, s. 143, 149–150.
[44] Ibid. s. 143.
[45] Limnéll, Jarno & Majewski Klaus & Salminen Mirva. *Kyberturvallisuus*, Docendo Oy, Jyväskylä 2014, s. 13–26.
[46] Sivonen, Pekka. Personligt samtal 27.6.2014.
[47] Ordet traditionella syftar på säkerhetsteorier som realism och liberalism.
[48] Emmers, R. (2010) “Securitization”, s. 138.

Detta leder till att objekten för säkerhetspolitiken också är annorlunda. I detta fall kan objekten vara individer, samfund eller ekonomin.[49] Dessa är element som ofta förekommer i nationella cybersäkerhetsstrategier[50].

När det kommer till nationell cybersäkerhetspolitik säger Ronald Deibert, professor vid Canada Centre of the Global Security, att stater allt oftare borde ställa frågorna: ”*security from whom*?” (säkerhet från vem?) och ”*security for what*?” (säkerhet för vad?), istället för att se cybersäkerheten som ett traditionellt säkerhetsproblem[51]. Dessa frågeställningar är kopplade till den säkerhetslogik som Jarno Limnéll nämner i sin avhandling, då han talar om vad hotbildspolitik och säkerhetisering innebär[52]. Limnéll är av den åsikten att detta hör till grundfrågorna som måste ställas då en säkerhetsstrategi utarbetas[53].

Trots att säkerhetiseringen är en fungerande referensram, ger den tyvärr inte svar på alla frågor. Det största problemet är att veta när ett ärende är ett normalt politiskt ärende och när det är ett säkerhetiserat ärende[54]. Enligt Emmers innebär detta handlingar, som avviker från de vardagliga politiska förfarandena[55]. Limnéll poängterar att åtgärderna kan variera beroende på säkerhetsområdet[56]. I frågan om cybersäkerhet, skulle det kunna handla om att en mängd ekonomiska resurser frigörs eller att lagstiftningsförändringar motiveras[57].

Ett annat kriterium, för en säkerhetisering, är att hotet på något sätt bör utgöra ett ”*existentiellt hot*” för ett utvalt referensobjekt[58]. Därför kommer detta arbete att söka efter faktorer i Finlands och Sveriges cybersäkerhetspolitik som indikerar att cyberhoten uppfattas som ett hot mot samhället och dess vitala funktioner. Detta innebär att ländernas hotbilder analyseras. Därpå kommer undersökningen att analysera vad länderna är redo att göra för att avvärja hoten, vilket samtidigt är en del av målen för ländernas säkerhetisering.

---

[49] Emmers, R. (2010) “Securitization”, s. 138.
[50] OECD (2012) “Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy”, s. 1–28.
[51] Deibert, Ronald. “Divide and Rule: Republican Security Theory as Civil Society Cyber Strategy”, Famularo, Julia M. & Kepe, Marta. (ed.), *International Engagement on Cyber III: State Building on a New Frontier*, Georgetown Journal of International Affairs, Institute for Law, Science & Global Security, Washington 2013, s. 39–49.
[52] Limnéll, J. (2009) *Suomen uhkakuvapolitiikka 2000-luvun alussa*, s. 46.
[53] Jarno Limnéll. Intervju 7.4.2014.
[54] Emmers, R. (2010) “Securitization”, s. 143.
[55] Ibid. s. 141.
[56] Limnéll, J. (2009) *Suomen uhkakuvapolitiikka 2000-luvun alussa*, s. 73.
[57] Limnéll, Jarno. Intervju 7.4.2014.
[58] Emmers, R. (2010) “Securitization”, s. 140.

Som nämnt, kan också en motiverad förändring av lagstiftning vara målet för en säkerhetisering. Didier Bigo skriver att säkerhetiseringsteorierna bättre beaktar ”*lag och ordning*” än var traditionella säkerhetsstudier gör[59]. Detta är en viktig detalj med tanke på den lagstiftningsanalys som denna studie strävar efter. Bigo skriver att: säkerhetiseringen, ur det juridiska perspektivet, ämnar skapa trygghet samt juridiska och rättsliga garantier för individen i samhället. Detta passar ihop med de rättsprinciper som delvis återges i Sveriges regeringsform[60] och Finlands statsskick[61].

Om de juridiska aspekterna inte tas i beaktande kan det i värsta fall leda till oro bland medborgarna. Enligt Bigo, är målet med en säkerhetisering alltid att lugna och skapa förtroende hos medborgarna.[62] Ifall målet med säkerhetiseringen är att påverka lagstiftningen, betyder det att förändringen måste resultera i regelverk som garanterar individens mänskliga och grundläggande rättigheter, och som noggrant definierar myndigheternas befogenheter.[63]

Bigo tillägger att en säkerhetisering också innebär uppoffringar. Han säger att det alltid finns vinnare och förlorare i en säkerhetiseringsprocess; någons säkerhet måste uppoffras för att något annat skall kunna prioriteras. [64] Säkerhet kommer därför alltid med en *alternativkostnad*[65]. Säkerhetiseringens slutresultat beror därför ofta på utförd politik och legitimeringsstrategi. Därmed har den anförda terminologin en central roll då säkerhetiseraren försöker motivera praktiserandet av övervakning, kontroll och bestraffning.[66] Svårigheten är att, som utomstående, kunna säga vad som egentligen uppoffras i kampen mot de nya säkerhetshoten[67]. Detta arbete kommer inte att kunna analysera vad som uppoffras, utan konstaterar endast att skapandet av säkerhet alltid kräver politisk vilja och ekonomiska resurser.

Därmed är ansatsen för denna undersökning att Finland och Sverige säkerhetiserar sin cybersäkerhetsagenda för att motivera sin närvaro som säkerhetsaktörer i cyberrymden.

---

[59] Bigo, D. (2008) “International Political Sociology”, s. 122.
[60] *Sveriges regeringsform*, lag (2002:903), 1 kap. 2§, 1–2 mom.
[61] *Finlands grundlag*, lag (11.6.1999/731), 1 kap. 1§, 2 mom.
[62] Bigo, D. (2008) “International Political Sociology”, s. 122–123.
[63] *Finlands grundlag*, 1 kap. 1§, 2 mom. & *Sveriges regeringsform*, 1 kap. 2§, 1–2 mom.
[64] Bigo, D. (2008) “International Political Sociology”, s. 122–123.
[65] Zakheim, Dov S. “The Opportunity Cost of Security”, *Prism*, Vol. 3, No.3, 2014, s. 119–124. [http://cco.dodlive.mil/files/2014/02/prism119-124_zakheim.pdf / 1.3.2014]
[66] Bigo, D. (2008) “International Political Sociology”, s. 123.
[67] Jarno Limnéll analyserar detta i sin avhandling: *Suomen uhkakuvapolitiikka 2000-luvun alussa* genom att jämföra statsrådets principbeslut från olika regeringsperioder.

3 TIDIGARE FORSKNING OCH UTÖVAD CYBERSÄKERHETS-POLITIK

Med hjälp av officiella politiska utlåtanden[68] försöker stater skapa en bild av *”sanning, värdighet och kontinuitet*” för den utförda cybersäkerhetspolitiken.[69] Samtidigt kan det uppfattas som en strävan att nå de politiska målsättningarna genom säkerhetisering.[70] Utlåtandena kan också innehålla sekundära intressen, som att gynna landets näringsliv och ekonomi, genom att trygga en säker och förutsägbar verksamhetsmiljö för företag[71].

Det finns ett flertal källor som behandlar cyberfrågor. Däremot finns det få jämförande studier av cybersäkerhetsstrategier. Den mest betydande jämförande undersökningen är OECDs rapport från år 2012. En kort genomgång av denna rapport följer härefter.

Efter denna genomgång, kommer undersökningen att analysera Finlands och Sveriges statliga dokument som formar cybersäkerhetspolitiken. Som tidigare nämnt, saknar Sverige en officiell cybersäkerhetsstrategi. Sverige har dock gett ut motsvarande dokument som de bygger sin cybersäkerhetspolitik på. Dessa dokument kommer att utgöra centrum för denna studie.

3.1 OECDs rapport

Till skillnad från denna studie är OECDs rapport variabelbaserad, vilket betyder att den jämför ett antal förutvalda faktorer. Rapporten ger läsaren en generell överblick av vad olika länder har kommit fram till, men analyserar inte strategiernas styrkor och svagheter desto mera. I boken *Kyberturvallisuus* skriver Limnéll, Majewski och Salminen att olika länders strategier sällan avsevärt skiljer sig från varandra[72], vilket också i detta fall är väntevärdet för slutsatserna av OECDs rapport.

OECDs rapport konstaterar att samhällen, deras ekonomier och administration är beroende av ett väl fungerande Internet och att cybersäkerhet därför allt mera blivit en nationell prioritet.[73] Rapporten visar att de jämförda länderna ser lika på cybersäkerhetens roll för ekonomin, utbildningen och samhället. En trend är att cybersäkerheten utvecklats till en balansgång mellan

[68] Cybersäkerhetsstrategierna hör till dessa. Jarno Limnéll. Intervju 7.4.2014.
[69] Limnéll, J., Majewski K. & Salminen M. (2014) *Kyberturvallisuus*, s. 83.
[70] Limnéll, J. (2009) *Suomen uhkakuvapolitiikka 2000-luvun alussa*, s. 72–73.
[71] Limnéll, J., Majewski K. & Salminen M. (2014) *Kyberturvallisuus*, s. 58–62.
[72] Ibid. s. 83
[73] OECD (2012) “Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy”, s. 1–57.

nationella säkerhetsintressen och Internet, som en kanal för innovation, yttrandefrihet och ekonomisk tillväxt. Det positiva är att cybersäkerheten i de flesta länder stöds av ett starkt politiskt ledarskap, vilket förbättrar den politiska beslutsfattningsförmågan.[74]

De jämförda länderna ser också lika på hoten. Rapporten lyckas trots detta inte identifiera gemensamma juridiska definitioner på cyberterminologin eller allmänt accepterade åtgärder som en nation får vidta för att avvärja cyberhoten.[75]

När det kommer till lagstiftningen, är trenden att de flesta nationer poängterar internationellt samarbete. Detta samtidigt som cybersäkerheten i samtliga länder.[76] OECDs rapport föreslår att man borde undersöka vilka ekonomiska- och samhällsområden som kunde ingå i det internationella samarbetet, samtidigt som länderna borde ändra på självständighetstänkandet i cybersäkerhetsfrågor. Ett problem är att samarbete hittills endast har skett på den tekniska nivån. Enligt rapporten är lösningen på problemet att utvidga samarbetet till att även omfatta den operativa nivån.[77]

3.2 Finland: Statsrådets säkerhets- och försvarspolitiska redogörelse

Statsrådets säkerhets- och försvarspolitiska redogörelse är det mest betydande finska säkerhetspolitiska dokumentet, eftersom redogörelsen utgör regeringens riktlinjer för den finländska säkerhetspolitiken[78]. Här definierar Finland på en generell nivå vad som hotar samhället och hur man tänker fördela resurser för att svara på hoten, samtidigt som det uttrycker beslutfattarnas politiska vilja.[79] På så sätt är redogörelsen den högsta säkerhetspolitiska kommunikationskanalen för beslutsfattarna och samtidigt en talesakt.

I sin doktorsavhandling skriver Jarno Limnéll att statsmakten inte nödvändigtvis måste applicera några politiska nödåtgärder för att säkerhetisera sin politiska agenda. Han anser det vara tillräckligt att beslutsfattarna lyfter upp något som ett hot mot säkerheten i ett officiellt doku-

[74] OECD (2012) "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", s. 1–57.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Finlands statsråd, *Redogörelse om Finlands säkerhets- och försvarspolitik till riksdagen*, 20.12.2012. [http://vnk.fi/ajankohtaista/tiedotteet/tiedote/sv.jsp?oid=373201 / 19.5.2014]
[79] Koivula, Tommi. Proseminarium 7.5.2014.

ment. Enligt honom är *Statsrådets säkerhets- och försvarspolitiska redogörelse* ett sätt att säkerhetisera.[80]

I redogörelsen från år 2009 lyfter Finland för första gången fram attacker via Internet som ett hot mot säkerheten. Då i samband med terrorhot.[81] En tydlig utveckling går att märka då man jämför redogörelsen från 2009 med redogörelsen från 2012. Jämförelsen visar att cybersäkerheten på tre år har fått en mycket större prioritet i den finländska säkerhetspolitiken.[82] Till näst är en sammanfattning som visar på vilket sätt *Statsrådets säkerhets- och försvarspolitiska redogörelse* för tillfället behandlar cybersäkerheten.

I sammanfattningen av redogörelsen från år 2012 lyfter statsrådet fram samhällets beroende av teknologi som en sårbarhet. Bland annat trafiken, kommunikationen och energiförsörjningen är beroende av tekniska nätverk. Därmed riktas fokus på att utveckla cybersäkerheten, för att skydda samhällets vitala funktioner.[83]

Statsrådets redogörelse (2012) lyfter också fram cyberattacker som ett asymmetriskt hot, vid sidan om terrorism och icke statlig användning av så kallade CBRN (kemiska, biologiska, radioaktiva och kärn-) vapen. Statsrådets redogörelse sammanfattar att man måste förbereda sig och förebygga dessa asymmetriska hot. Vilka resurser som kommer att utdelas för avvärjandet av cyberhot, nämns inte här.[84]

Redogörelsen betonar det internationella samfundets roll vid lösandet av cybersäkerhetsproblem. Detta har visat sig vara svårt, då olika länder har olika ekonomiska och säkerhetspolitiska intressen. En annan fråga som delar åsikterna globalt är synen på mänskliga rättigheter och statens roll i förhållande till individens frihet.[85]

Statsrådets redogörelse nämner också att cyberattacker kan vara en del av den framtida krigsföringen, som kan användas för politisk och ekonomisk utpressning. Attackerna riktas mot hela samhället och det blir i framtiden allt svårare att spåra upp attackens ursprung.[86] Redogö-

[80] Limnéll, J. (2009) *Suomen uhkakuvapolitiikka 2000-luvun alussa*, s. 73–76.
[81] *Finlands säkerhets- och försvarspolitik 2009*, SRR 1/2009 rd.
[82] Jämför: *Finlands säkerhets- och försvarspolitik 2009* och *Finlands säkerhets- och försvarspolitik 2012*. Statsrådets redogörelse till riksdagen 20.12.2012, SRR 6/2012 rd, Helsingfors 2012.
[83] *Finlands säkerhets- och försvarspolitik 2012*, SRR 6/2012 rd, s. 10–11.
[84] Ibid. s. 21.
[85] Ibid. s. 22.
[86] Ibid. s. 36–37.

relsen föreslår att man borde bilda ett gemensamt nordiskt nätverk, som skulle diskutera cybersäkerhets frågor.[87]

En lyckad cybersäkerhetspolitik kräver för Finlands del ett brett internationellt samarbete, centraliserade lösningar och en organiserad lägesbildsverksamhet[88]. För att lyckas med detta har Finland år 2013 fastställt en nationell cybersäkerhetsstrategi, som skall skapa grunden för en organiserad verksamhet. Därpå har Finland utarbetet ett verkställighetsprogram för cybersäkerhetsstrategins, som berättar hur man skall nå de strategiska målen.[89] Med tanke på militära förmågor, nämner *Statsrådet säkerhets- och försvarspolitiska redogörelse* att man på lång sikt måste satsa resurser på upprätthållandet och byggandet av kapacitet som: *"cyber- och elektronisk krigsföring, fjärrverkande vapen och mobilitet"*[90]. Detta visar att Finland är redo att ge cybersäkerhetsarbetet utökade ekonomiska medel.

3.3 Finland: Säkerhetsstrategi för samhället

Säkerhetsstrategi för samhället är en strategi vars mål är att konkretisera den försvarspolitiska redogörelsens (2009) principer och mål till handlingsmodeller. Den är gjord på uppdrag av Finlands statsråd år 2010 och är därför en hög politisk status. Strategin har inte lika hög politiskprioritet som *Statsrådet säkerhets- och försvarspolitiska redogörelse*, men är ändå en del av den säkerhetspolitiska stommen.[91]

Meningen med strategin är att utgöra en gemensam grund för beredskap och krisledning, för alla aktörer i samhället. Den berör således alla myndigheter då den försöker koordinera myndigheternas fungerande och samarbete under en krissituation.[92] Strategin ger en bra bild av de vitala samhällsfunktionerna som är beroende av cyberdomänet samt myndigheternas roll.

För att möjliggöra ledandet i en krissituation, ansvarar statsrådets kansli för upprätthållandet av en aktuell lagstiftning, samt för utrymmena och den tekniska utrustningen. Likaså upprätthåller statsrådets ledningscentral beredskap, så att den kan stöda statsledningen under alla om-

[87] *Finlands säkerhets- och försvarspolitik 2012*, SRR 6/2012 rd, s. 67.
[88] Ibid. s. 94–95.
[89] Säkerhetskommittén, *Cybersäkerhetsstrategins verkställighetsprogram*, [http://www.turvallisuuskomitea.fi/index.php/sv/kyberturvallisuusstrategia/toimeenpano-ohjelma / 24.5.2014]
[90] *Finlands säkerhets- och försvarspolitik 2012*, SRR 6/2012 rd, s. 110.
[91] Finlands försvarsministerium. *Säkerhetsstrategi för samhället*. Statsrådets principbeslut 16.12.2010, Helsingfors 2010, s. 1.
[92] Finlands statsråd, *Säkerhetsstrategi för samhället*, 16.12.2010. [http://vnk.fi/toiminta/turvallisuus/YTS/sv.jsp / 19.5.2014]

ständigheter.[93] Detta kan tolkas som en handling av säkerhetisering, eftersom Finland spenderar resurser på hotbilder som ännu inte har konkretiserats. Säkerhetsstrategin nämner dock inte hur mycket resurser som staten tänker öronmärka, för avvärjandet av eventuella cyberhot.

Enligt avsnittet om behandling av eventuella störningssituationer, ansvarar den behöriga myndigheten för den operativa ledningen. Målet är att andra myndigheter vid behov skall kunna ge en handräckning till varandra. Om krisen fördjupas, kommer hjälpen från ministeriet och i sista hand från statsrådet, som leds av statsministern.[94] Detta betyder att varje enskild myndighet och företag själv måste vara beredd på att bygga upp sitt cyberförsvar[95]. Svagheten med en delad ledning är att motåtgärderna ofta börjar för sent[96].

Enligt Antti Pirinen, Tietoturva ry:s ordförande och KPMG:s datasäkerhetschef, är denna handlingsmodell ändå ett seriöst alternativ[97]. Han säger, att det krävs en harmonisering av resurser, så att varje myndighet känner till varandras system. Enligt Pirinen kräver det därtill en instans som uppehåller och övervakar datasystemens säkerhetsinställningar[98]. Säkerhetsstrategin för samhället nämner inte om staten kommer att bidra med extra medel för att åstadkomma förändringarna, eller om myndigheterna måste nöja sig med de befintliga medlen.

Antti Pirinen fortsätter med att säga att det är nödvändigt att upprätthålla en lägesbild i realtid under alla omständigheter.[99] Säkerhetsstrategin konstaterar att lägesmedvetenheten stöder ledandet och förenklar koordinering i en eventuell krissituation. Lägesbildsverksamheten utvecklas genom att utnyttja och tillgodogöra de datatekniska ekosystem som redan existerar.[100] För upprätthållandet och delandet av lägesbilden har Finland valt att grunda ett cybersäkerhetscenter[101].

Kommunikationen nämns även som en central del av *Säkerhetsstartegin för samhället*. Finland kommer att vidareutveckla nättjänstsystemen och införa en medborgarportal. Statsför-

---

[93] Finlands statsråd, *Säkerhetsstrategi för samhället*, 16.12.2010. [http://vnk.fi/toiminta/turvallisuus/YTS/sv.jsp / 19.5.2014]
[94] Ibid.
[95] Catharina Candolin, Intervju 7.2.2014.
[96] Kasvi, Jyrki. *Strategia joka katosi*, blogginlägg 24.1.2013, YLE nyheter, [http://yle.fi/uutiset/jyrki_kasvi_strategia_joka_katosi/6465713 / 4.7.2014]
[97] Antti Pirinen. Intervju 11.7.2014.
[98] Ibid
[99] Ibid.
[100] Finlands försvarsministerium (2010) *Säkerhetsstrategi för samhället*, s. 22.
[101] Säkerhetskommittén. *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*. 11.3.2014, Helsingfors 2014, s. 11–12.

valtningen kommer också att utbilda personal för kriskommunikation.[102] Detta tyder på att Finland är villig att satsa resurser på kapacitet som indirekt är kopplade till cybersäkerheten.

3.4 Finland: Strategi för cybersäkerheten i Finland

För att utveckla cybersäkerheten vidare har Finland publicerat *Strategin för cybersäkerheten i Finland*. Finlands försvarsministerium publicerade strategin år 2013, som ansvarsmyndighet för Finlands säkerhet.[103] Strategin behandlar inte endast den militära cybersäkerheten, utan också den cybersäkerhet som berör Finlands interna och fredstida säkerhet. Strategin kan uppfattas som en fortsättning på *Statsrådets säkerhets- och försvarspolitiska redogörelse 2012* och *Säkerhetsstrategin för samhället*, men utgör samtidigt en helt egen politisk agenda. Strategin visar de politiska målen för Finlands cybersäkerhetspolitik, då den ger riktlinjer för hur Finland borde utveckla sin cybersäkerhet. Detta är ett praktexempel på Finlands sätt att säkerhetisera sin cybersäkerhetsagenda.

Det viktigaste målet enligt strategin är att skapa förutsättningar för en välfungerande cyberomgivning, vilket skulle gynna Finlands konkurrenskraft och ekonomiska möjligheter. Detta skulle ske genom att Finland skulle vara ett attraktivare investeringsobjekt för internationella företag och för att företag som redan fungerar i Finland enklare skulle kunna planera sin verksamhet.[104]

I strategin berättas hur Finland skall svara på cyberomgivningens utmaningar och se till att den fungerar. Utöver detta, beskriver strategin Finlands vision, handlingsmodell och riktlinjer för cybersäkerheten. Tanken är, i första hand, att trygga samhällets vitala funktioner, men också att cybersäkerheten skall täcka hela samhället. Detta skall ske genom ett ökat myndighetssamarbete och en utbildning som implementeras på alla utbildningsnivåer.[105]

Finland betonar tydligt att alla förändringar måste ske så att de grundläggande friheterna och rättigheterna tryggas, under alla omständigheter. Därtill betonar Finland informationsskydd, samt skydd för medborgarnas integritet och yttrandefrihet.[106]

---

[102] Finlands försvarsministerium (2010) *Säkerhetsstrategi för samhället*, s. 19–22.
[103] Finlands försvarsministerium, *Strategi för cybersäkerheten i Finland*, [http://www.defmin.fi/sv/publikationer/strategidokument/strategi_for_cybersakerheten_i_finland / 18.4.2014]
[104] Ibid.
[105] Ibid.
[106] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 33–35.

Bakgrundspromemorian tar ställning till ledningen av cybersäkerheten och arrangemang för hanteringen av störningssituationer[107]. Detta är en fortsättning på de riktlinjer som finns i *Säkerhetsstrategin för samhället*[108]. Tanken är att varje myndighet ansvarar för sitt eget verksamhetsområde och får vid behov stöd av de andra myndigheterna. Catharina Candolin, doktor i teknik och dataadministrationschef vid huvudstaben, anser att detta leder till en splittrad ledning och är därmed ett problem[109]. Enligt Limnéll är detta typiskt då den politiska ledningen gör hotbildspolitik[110]. Detta kan antingen bero på att de olika aktörerna inte villiga att ge upp sitt självstyre eller det upplevs som en börda att vara tvungen att sörja om andras säkerhet[111].

Cybersäkerhetscentret, som är en del av Kommunikationsverket, ansvarar för upprätthållande av en *”tillförlitlig och aktuell lägesbild”*.[112] Catharina Candolins åsikt är att cybersäkerhetscentret uppgifter borde definieras, så att det skulle skapa en centraliserad ledning. Hennes åsikt är att ledningen för tillfället är för utspridd.[113]

Jyrki Kasvi, doktor i teknik och utvecklingschef på Finska dataförbundet r.f., är av samma åsikt som Candolin, då han i sitt blogginlägg på Rundradions hemsidor skriver att en av de största bristerna i strategin är frånvaron av en centraliserad ledning. Som andra brister nämner han politikernas ovillighet att ge myndigheterna rätt till övervakning och underrättelse i cyberrymden. Han sammanfattar att de varierande politiska intressena har resulterat i en mager kompromiss.[114] Nyheterna om att cybersäkerhetsstrategin kom ut försenat, på grund av osämja mellan olika partier, stöder delvis detta argument[115]. Limnéll kostaterar dock sin doktorsavhandling att förväntningsvärdet i en säkerhetiseringsprocess är en godtagbar konsensus, eftersom de olika parterna objektivt strävar att definiera de rätta hotbilderna.[116].

Candolin kritiserar också strategin för att den inte uppmärksammar näringslivet tillräckligt starkt, med tanke på hur stort ansvar de har för den kritiska infrastukturen. Hon anser bland

---

[107] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 33–35.
[108] Finlands försvarsministerium (2010) *Säkerhetsstrategi för samhället*, s. 14–17.
[109] Catharina Candolin. Intervju 4.2.2014.
[110] Jarno Limnéll, Intervju 7.4.2014.
[111] Ibid.
[112] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 5
[113] Catharina Candolin. Intervju 4.2.2014.
[114] Kasvi, Jyrki. *Strategia joka katosi*, blogginlägg 24.1.2013, YLE nyheter, [http://yle.fi/uutiset/jyrki_kasvi_strategia_joka_katosi/6465713 / 4.7.2014]
[115] Helsingin Sanomat 18.1.2013, *Verkkohyökkäyksistä leimahti kiistahallituksessa*. [http://www.hs.fi/kotimaa/a1358401486659 / 18.3.2015]
[116] Limnéll, J. (2009) *Suomen uhkakuvapolitiikka 2000-luvun alussa*, s. 69.

annat att näringslivet starkare borde ha representerats i arbetsprocessen.[117] Antti Pirinen är inte förvånad att näringslivet inte har haft någon större roll i strategiarbetet, eftersom statens roll är att skydda de statliga nätverken. Han uttrycker ändå att HAVARO och Försörjningsberedskapscentralens samarbete med företagen, som styr den kritiska infrastrukturen, är tillräckliga stödåtgärder. Han fortsätter med att säga, att myndigheterna bäst kan stöda näringslivet genom en förutsägbar lagstiftning som är i kraft över 5 år åt gången och genom att bidra med en instans, vart företagen anonymt kan meddela om upptäckta säkerhetshot i sina egna eller andras nätverk.[118]

3.5 Finland: Verkställighetsprogrammet för cybersäkerhetsstrategin

På samma sätt som *Säkerhetsstrategi för samhället* är en fortsättning på *Statsrådets säkerhets- och försvarspolitiska redogörelse* är också *Verkställighetsprogrammet för cybersäkerhetsstrategin* är en fortsättning på cybersäkerhetsstrategin[119]. Verkställighetsprogrammet publicerades år 2014 och är skrivet av Säkerhetskommittén på uppdrag av försvarsministeriet. Ur verkställighetsprogrammet framgår de konkreta åtgärder som Finland måste göra för att nå sina strategiska mål.[120] Åtgärderna är intressanta för denna undersökning eftersom de berättar vad som är Finlands mål för säkerhetiseringen av cybersäkerheten.

Verkställighetsprogrammet är mera omfattande än själva cybersäkerhetsstrategin. På säkerhetskommitténs webbplats berättas att ”*verkställighetsprogrammet påskyndar realiserandet av cybersäkerhetsstrategin*”[121]. Verkställighetsprogrammet ger samtidigt förutsättningar att evaluera säkerhetiseringsprocessen.

Verkställighetsprogrammet tar på en bred front ställning till vad som borde göras för att nå de strategiska målsättningarna. Programmet lyfter fram 74 konkreta åtgärder, varav de viktigaste utvecklingsobjekten är:

- cybersäkerhetscentret
- staten ska bedriva dataskyddsverksamhet dygnet runt

[117] Catharina Candolin. Intervju 4.2.2014.
[118] Kasvi, Jyrki. *Strategia joka katosi*, blogginlägg 24.1.2013, YLE nyheter, [http://yle.fi/uutiset/jyrki_kasvi_strategia_joka_katosi/6465713 / 4.7.2014]
[119] Säkerhetskommittén, *Cybersäkerhetsstrategins verkställighetsprogram*, [http://www.turvallisuuskomitea.fi/index.php/sv/kyberturvallisuusstrategia/toimeenpano-ohjelma / 24.5.2014]
[120] Säkerhetskommittén, *Cybersäkerhetsstrategins verkställighetsprogram*, [http://www.turvallisuuskomitea.fi/index.php/sv/kyberturvallisuusstrategia/toimeenpano-ohjelma / 24.5.2014]

- ett tjänsteintegreringsprojekt för hemlig dataöverföring och förvaltningens säkerhetsnät (SATU)
- polisens handlingsförmåga vid bekämpningen av cyberkriminalitet
- utvecklande av den lagstiftning som anknyter till cyberomgivningen och cybersäkerheten
- forsknings- och utbildningsprogram och annan förstärkning av kompetens[122]

Vid jämförelse med Sveriges cybersäkerhetspolitik är de tre sista punkterna de mest intressanta.

Verkställighetsprogrammet är rätt så myndighetscentrerat, trots att näringslivet och de enskilda medborgarna utgör den största användargruppen i cyberrymden. Enligt säkerhetskommittén stärks de andra aktörernas roll, då verkställandet av cybersäkerhetsstrategin framskrider, samt genom fortbildning och forskning.[123]

Enligt verkställighetsprogrammet måste varje nation få använda alla maktmedel, inom ramen för den internationella lagstiftningen, vid skyddandet av kritisk infrastruktur som hör till statens ansvarsområde. Förundersökningsmyndigheten bör ha tillräckliga befogenheter för att utreda brott som äger rum i cyberomginingen. I detta fall är det dock viktigt att yttrandefriheten och grundrättigheterna inte begränsas.[124]

För att utveckla lagstiftningen, har justitieministeriet tillsatt en grupp som skall verkställa EU:s direktiv om *angrepp mot nationella informationssystem*[125]. Målet med direktivet är att föra medlemsländernas strafflagstiftning närmare varandra, när det handlar om angrepp mot nationella informationssystem[126].

Enligt Antti Pirinen har verkställighetsprogrammet en bra möjlighet att stöda den nationella cybersäkerheten. Han är därför intresserad av att se hur bra Finland lyckas implementera de föreskrivna åtgärderna. Genomförandet av åtgärderna betyder samtidigt att en mängd ekono-

[122] Säkerhetskommittén (2014) *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma.*, s. 2.
[123] Ibid. s. 3–4.
[124] Ibid.
[125] Ibid.
[126] Europaparlamentet, Europaparlamentets lagstiftningsresolution 2010/0273(COD), 4.7.2013. [http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0321&language=SV&ring=A7-2013-0224 / 1.7.2014]

miska resurser måste frigöras. Hur betydande lagstiftningsåtgärderna kommer att bli återstår enligt honom att se.[127]

3.6 Sverige: Strategi för samhällets informationssäkerhet

Som tidigare nämnts, har Sverige inte någon officiell cybersäkerhetsstrategi. Sveriges motsvarighet till Finlands cybersäkerhetsstrategi heter *Strategi för samhällets informationssäkerhet*. Denna strategi utgavs våren 2011 av Myndigheten för samhällsskydd och beredskap.[128] Som statligt dokument har strategin inte samma politiska status som *Statsrådets säkerhets- och försvarspolitiska redogörelse*, utan det politiska värdet kommer från att strategin är utgiven av en myndighet som fått sin makt av regeringen[129]. Själva arbetsprocessen påminner om den arbetsprocess som Finlands cybersäkerhetsstrategi genomgått, i och med att Myndigheten för samhällsskydd och beredskap (MSB), tillsammans med Försvarets radioanstalt (FRA), Försvarsmakten (FM), Försvarets materialverk samt Post- och telestyrelsen alla varit med om att utarbeta strategin.[130]

Strategin visar på vilket sätt Sverige säkerhetiserar sin cybersäkerhetsagenda. För att lyckas med utmaningar inom informationssäkerhet anser Sverige att det behövs en gemensam uppfattning om informationssäkerhetsarbetet. Strategin tar därför bland annat ställning till strukturen för myndighetssammarbete.[131] Utredningen är indelad i fem delområden och de konkreta målen och åtgärderna för hur de strategiska målen skall uppnås, hittas i den nationella handlingsplanen.[132] Det är intressant att märka att Sverige i och med detta har valt att behandla cybersäkerheten som en del av informationssäkerheten. Detta har lett till att cybersäkerheten endast behandlas på ett allmänt plan i strategin.[133] Informationssäkerhetsstrategin fokuserar också starkt på interna säkerhetsfrågor, trots att också Försvarsmakten varit med i det strategiska arbetet[134]. Detta är en intressant skillnad jämfört med Finland.

I första hand är syftet med strategin är att skapa långsiktiga målsättningar och riktlinjer för arbetet kring Sveriges informationssäkerhet. Det primära målet är att skapa en gemensam för-

[127] Antti Pirinen. Intervju 11.7.2014.
[128] Myndigheten för samhällsskydd och beredskap. *Strategi för samhällets informationssäkerhet 2010-2015*, Stockholm 2010.
[129] Myndigheten för samhällsskydd och beredskap (MSB), webbplats. [https://www.msb.se / 24.2.2015]
[130] MSB (2010) *Strategi för samhällets informationssäkerhet 2010-2015*, s. 3.
[131] Ibid.
[132] Ibid., s. 5.
[133] Ibid. s. 5–10
[134] Ibid. s. 3

ståelse för informationssäkerhet bland beslutsfattare, myndigheter och näringslivet. I andra hand, är strategin riktad till den vanliga medborgaren. Den är menad att, tillsammans med den nationella handlingsplanen för krissituationer, ge riktlinjerna för Sveriges informationssäkerhet.[135] Även om informationssäkerhetsstrategins primära mål inte är att säkerhetisera cybersäkerheten, beaktar den ärenden som är relaterade till cybersäkerhetsfrågor.

Sverige ser informationssäkerhet som en viktig del i strävan att *”nå kvalitets- och effektivitetskrav för olika processer”*[136]. Säkerhetsstrategin påpekar att en dålig informationssäkerhet kan ha följder som sträcker sig långt utanför själva säkerhetsområdet**.**[137] Som konkreta hot mot informationssäkerheten på Internet nämns bedrägeri, utpressning, förtal och sabotage. Man nämner också att dessa brott måste motverkas.[138] Vilka åtgärder detta innebär nämns inte i strategin. En annan nackdel är att strategin inte direkt tar ställning till de hot som enbart riktar sig mot statssäkerheten. Informationssäkerheten har dock gjorts till hela landets sak, då den hävdar att kunskapen om risker för användningen av elektronisk kommunikation måste läras ut redan i grundskolan och att inlärningen därefter skall fortsätta ända till högskole- och universitetsnivå.[139]

De största bristerna inom informationssäkerhet kan enligt MSB hittas i den mänskliga faktorn. Därför är det viktigt att satsa på ett ökat medvetande och kompetens inom området. I strategin nämns organisationsledningen för företag som en nyckelgrupp, eftersom de i slutändan ansvarar för verksamhetens kvalitet och säkerhet. De ansvarar också för beslutandet om operativa skyddsåtgärder. MSB föreslår att man borde starta en nationell forskning och forskarutbildning inom området för att uppehålla både generell- samt spetskompetens inom området.[140]

Strategin poängterar att det är viktigt att bygga fungerande nätverk för utbyte av kunskap och erfarenheter, mellan den privata och offentliga sektorn. På samma gång måste Sverige vara aktiv i den internationella medverkan. Strategin nämner EU och de övriga nordiska länderna samt enskilda stater som huvudsakliga samarbetspartner.[141]

---

[135] MSB (2010) *Strategi för samhällets informationssäkerhet 2010-2015*, s. 5–6.
[136] Ibid. s. 9–13.
[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] Ibid.
[141] Ibid.

En stor skillnad mellan Finlands cybersäkerhetsstrategi och Sveriges *Strategi för informationssäkerheten i samhället* är att Sverige inte målar upp hotbilder på samma sätt. Det ända hotbilderna som informationssäkerheten målar upp, nämns då strategin talar om de metoder som utgör de förebyggande åtgärderna. Strategin nämner här att hot mot den elektroniska informationssäkerheten kräver säkra kryptografiska funktioner och signalskydd och att den kritiska infrastrukturen, som bygger på elektronisk kommunikation, måste vara tillräckligt robust.[142] Strategin tar dock inte ställning till vilka åtgärder eller ekonomiska resurser detta innebär.

Strategin nämner till sist att det också krävs ramverk för evaluering och val av säkerhetsåtgärder, som bör fastställas både nationellt och internationellt.[143] Med tanke på säkerhetiseringens slutresultat, är det viktigt att följa med hurudana åtgärder detta kommer att leda till.

3.7 Sverige: Försvarshögskolans cyberrapport till regeringen

Med hjälp av den utredning som Sveriges Försvarshögskola gav regeringen år 2012, försöker man definiera och dra en linje mellan informations- och cybersäkerhet. Däröver har Försvarshögskolan, i sin rapport till regeringen, gett förslag på hur Sverige i framtiden kunde ta ställning till cybersäkerhetsfrågor.[144]

Rapporten går inte att analysera helt ur samma perspektiv som ett officiellt statligt dokument, därför att det inte är en del av den åt allmänheten synliga säkerhetiseringen. Rapporten är ändå en indikation på vilket sätt cybersäkerheten behandlas på den högsta säkerhetspolitiska nivån i Sverige. Således kan rapporten tolkas som Försvarshögskolans sätt att säkerhetisera cybersäkerheten, men inte direkt som statsmaktens officiella linje. Däremot ger rapporten en bra inblick i Sveriges sätt att göra cybersäkerhetspolitik och åt vilket håll cybersäkerhetspolitiken är på väg. Rapporten innehåller också information som berättar på vilket sätt Försvarshögskolan uppfattar cyberdomänen som ett existentiellt hot och vilka åtgärder som förespråkas.

Först och främst har cyberförsvarsrapporten kommit fram till att cyberterminologin måste definieras noggrannare. Samtidigt måste Sverige besluta huruvida begreppen skall relateras till sina internationella motsvarigheter. En möjlighet är att låta cybersäkerheten omfatta mera an-

[142] MSB (2010) *Strategi för samhällets informationssäkerhet 2010-2015*, s. 12.
[143] Ibid.
[144] Sveriges Försvarshögskola, *Rapport Cyberförsvar* (254/2012), bilaga 1. Försvarshögskolans rapport till regeringen 20.12.2012, Stockholm 2012, s. 2-3.

tagonistiska hot och låta informationssäkerhet stå kvar i sin nuvarande form. Rapporten hävdar också att informationssäkerheten borde fokusera mera på förebyggande åtgärder och cybersäkerheten på hanteringen av aktuella hot.[145]

Rapporten konstaterar att staten har få möjligheter att ingripa mot ett cyberangrepp som skulle slå ut kritisk infrastruktur, på grund av att de försvars- och säkerhetspolitiska utgångspunkterna är otydliga. Fastställda regelverk finns endast i en sådan situation, där cyberattacken är kombinerad med andra militära medel. Försvarshögskolan påpekar att det är av försvars- och säkerhetspolitisk betydelse att detta reds ut och att man bereder olika förslag för att lösa problemet. Försvarshögskolan anser det även vara nödvändigt att lyssna till näringslivet, då förslagen utreds.[146] Detta visar att Försvarshögskolan upplever cyberangreppen som allvarliga hot mot samhällssäkerheten.

Utredningen visar att risk- och sårbarhetsalanyser inom informationssäkerhet är outvecklade med tanke på hot och risker mot vitala samhällsfunktioner. Rapporten konstaterar att ansvarsfördelningen mellan myndigheter är entydig, men att regelverk, metoder och verktyg för att kunna hantera en nationell krissituation är outvecklade. Utöver detta, bör fortsatta utredningar gällande samarbete på regerings- och myndighetsnivå göras.[147]

Till förebyggande åtgärder mot cyberhot hör central samverkan och samordning mellan olika aktörer. För att förbättra detta krävs analys av lagstiftningen inom olika områden. Det viktigaste är att hitta lösningar för situationer som faller i gråzonen mellan krig och fred. Därmed är det viktigt att utreda vilket stöd Försvarsmakten kan och bör kunna ge det civila samhället, i form av underrättelsetjänst och *signalspaning*[148]. Fokus bör ligga på vilka myndigheter som får inhämta och utbyta information, och i vilka situationer. Lagstiftningen bör också beakta samutnyttjandet av myndighetsresurser.[149]

De privata aktörerna har också blivit beaktade i rapporten. Rapporten nämner att faktorer och lagstiftning, som påverkar och underlättar samarbetet mellan privata och offentliga aktörer inom området för cyberrelaterade frågor, bör utredas.[150]

---

[145] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 44–47.
[146] Ibid.
[147] Ibid.
[148] I Sverige används termen ”signalspaning” också för termerna ”nätövervakning” och ”nätspaning”, trots att det är en överkategori. Sigholm, J. Brevväxling 1.2.2014.
[149] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 45–47.
[150] Ibid. s. 46.

Vidare konstaterar rapporten att Sverige måste analysera möjligheter att tillämpa internationell rätt inom cyberdomänen. Samtidigt måste man analysera behovet av nya regelverk. En viktig fråga är vilka regelverk som skall tillämpas i fredstid och vilka som skall tillämpas under krisförhållanden. FN nämns som det främsta organet för utförandet av internationell lagstiftning.[151] Sverige anser att det internationella samfundet måste besluta hur FN-stadgans kap. VI och VII[152] skall tillämpas vid cyberattacker. Man måste också utreda hur cyberkapacitet kunde användas för att införa sanktioner.[153]

Sverige ser det som sin plikt att delta i det internationella samarbetet.[154] EU uppfattas som en viktig samarbetspartner för utvecklandet av gemensamma policyn och strategier, beträffande säkerhet på Internet. Däremot uppfattar inte Sverige EU, som en lika stark aktör vid agerande mot cyberattacker, som till exempel NATO.[155]

Sverige ser USA som den viktigaste enskilda samarbetspartnern, på grund av deras teknologiska försprång. En annan viktig samarbetspartner är Storbritannien, på grund av deras kostnadseffektiva lösningar och uppbyggnad av organisationen mellan den privata och offentliga sektorn. Rapporten hävdar att det är i Sveriges intresse att ansöka om medlemskap i NATOs *Co-operative Cyber Defence Center of Exellence* (CCD CoE).[156]

3.8 Sverige: It i människans tjänst - En digital agenda för Sverige

Ett tredje svenskt dokument, som är betydande för denna studie, är Sveriges digitala agenda. *It i människans tjänst - En digital agenda för Sverige* utgavs hösten 2011 av Sveriges näringsdepartement. Agendan är av högt politiskt värde eftersom det är ett ställningstagande av Sveriges regering åt vilket håll de vill styra it-politiken. I agendan talar Sverige om hur man vill utnyttja möjligheterna som digitaliseringen medför, för att möta nationella och internationella samhällsutmaningar.[157] Dokumentet är intressant för denna undersökning också därför att det

[151] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 47.
[152] FN-stadgar kap VI och VII berättar hur brott mot fred i första hand bör lösas och vilka andra åtgärder som kan vidtas. För mera information, se: Förenta Nationerna, *Förenta Nationernas stadga och stadga för den internationella domstolen*, 1945. [http://www.fn.se/PageFiles/1158/FN-stadgan.pdf / 17.3.2014], s. 7–10.
[153] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 46–47.
[154] Ibid.
[155] Ibid. s. 18.
[156] Ibid. s. 45.
[157] Sveriges näringsdepartement, regeringskansliet 6.10.2011. [https://www.regeringen.se/sb/d/14216/a/177256 / 24.2.2015]

är ett exempel på Sveriges sätt att göra cybersäkerhetspolitik. Trots att dokumentet inte explicit nämner cybersäkerheten som term, kräver uppnåendet av de mål som ställs att cybersäkerheten beaktas. Ett tecken på Sveriges säkerhetisering är att staten är redo att lägga resurser på utvecklandet av sina digitala nätverk.

Näringsdepartementets syfte med denna strategi är att samla alla pågående aktiviterer på ett och samma ställe, för att på så sätt kunna ta till vara alla de möjligheter som digitaliseringen erbjuder människor och företag.[158] Strategin konstaterar att utnyttjandet av digitaliseringens möjligheter kräver en roll av alla som använder elektroniska system. Arbetet måste vara långsiktigt, samtidigt som utvecklingen bör följas upp och analyseras. Sverige har därför beslutat att inrätta en digitaliseringskomission, vars uppgift just är att jobba för dessa mål.[159]

För att öka digitaliseringens möjligheter, är det viktigt att alla skall kunna använda de möjligheter som digitaliseringen erbjuder. Detta innebär enligt Sverige att man måste bygga ny infrastruktur, att systemen måste fungera felfritt, att internet och andra elektroniska tjänster måste vara lätta att använda och att staten måste bidra med tjänster som skapar mervärde.[160]

Sveriges IT- och energiminister, Anna-Karin Hatt, tackar den digitala agendan för att vara resultatet av ett brett samarbete mellan alla ministerier. Enligt henne har ingen process på regeringskansliet tidigare varit så öppen.[161] Det är förståeligt att agendan inte vållat någon kamp om resurser, då den inte delar ut några ansvarsområden eller befogenheter.

3.9 Sammanfattning och förutsägelser av kommande

De statliga dokumenten visar att Finland och Sverige har använt sig av olika metoder för att säkerhetisera sin cybersäkerhetsagenda och för att motivera sin närvaro som säkerhetsaktörer i cyberrymden. Resultaten indikerar att Finland mera målmedvetet strävar att säkerhetisera cybersäkerhetsbegreppet, medan Sverige ansett att cybersäkerheten kan behandlas under agendan för informationssäkerhet.

Analyserade dokument visar att länderna trots detta ändå ser ytterst lika på statens roll som väktare för lag och ordning, samt för medborgarnas grundläggande rättigheter och friheter i

[158] Sveriges näringsdepartement, *It i människans tjänst – en digital agenda för Sverige*. Stockholm 2011, s. 5–7.
[159] Ibid. s. 6
[160] Ibid.
[161] MSB (2010) *Strategi för samhällets informationssäkerhet 2010-2015*, s. 5.

cyberrymden. Finland och Sverige har också valt att integrera cybersäkerheten till en del av den övriga säkerhetspolitiken. På så sätt vill båda bygga upp en säkerhetsstruktur som grundar sig på demokrati och rättsstatsprinciper.

Trots att målen för cybersäkerhetspolitiken i respektive land är rätt lika, har länderna valt olika strategier. Finland försöker med hjälp av säkerhetiseringen motivera statens roll i cyberrymden på nytt, medan Sverige endast strävar att utveckla de säkerhetsstrukturer som redan existerar. För lagstiftningens del är ansatsen därmed att Finland med hjälp av säkerhetiseringen kommer att försöka ge myndigheterna nya befogenheter, samtidigt som Sverige försöker att anpassa lagstiftningen till den redan existerande säkerhetsstrukturen.

4 LAGSTIFTNINGEN SOM SÄKERHETSPOLITISKTVERKTYG

Cybersäkerheten har hittills, till en stor del, fokuserat och byggt på den tekniska utvecklingen. Därmed har strategi- och lagstiftningsfrågorna blivit efter.[162] Lagstiftningen har en central roll i cybersäkerhetspolitiken, eftersom den dikterar vad myndigheterna får göra, hur stark kontroll de har och sist och slutligen deras roll i cyberdomänen.[163] För att kunna trygga medborgarnas grundfriheter och integritet, bör lagstiftningen diktera myndigheternas befogenheter[164]. Historiska exempel visar att det i andra fall kan det ske missbruk av privat information[165].

En utmaning är cyberdomänens brokighet. Eftersom cybersäkerhet handlar om all sorts elektronisk verksamhet, allt från konfidentiella dokument och uppehållande av kritisk infrastruktur till brevväxling och virtuell underhållning i ett och samma nätverk, är det enligt Sveriges Försvarshögskola svårt att skapa en enhetlig lagstiftning. Detta gör att lagstiftningen samtidigt måste vara tillräckligt generell för att täcka så mycket som möjligt, men samtidigt vara tillräckligt skarp för att kunna skydda personlig integritet och kritisk infrastruktur.[166]

Enligt Johan Sigholm är ett problem att ämnet i sig är så nytt; hoten och metoderna är så nya att lagstiftningen ännu inte är anpassad till dem. Det är svårt att utföra lånsiktig lagstiftning då hoten och anfallsmetoderna konstant förändras.[167] Det har visat sig vara svårt för stater att försvara sig mot cyberhot om de juridiska regelverken inte är definierade, trots att teknisk kapacitet och kunnande redan finns[168].

Det som redan nu är säkert är att lagstiftningsfrågorna i slutändan måste lösas på en internationell nivå, då cyberdomänen sträcker sig över de nationella gränserna[169]. Också beslutsfattarna runtom i världen har insett att det är nödvändigt att komma överens om gemensamma

---

[162] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 36.
[163] Catharina Candolin. Intervju 7.2.2014.
[164]Finlands statsråd, *Försvarsminister Haglund tillsatte en arbetsgrupp för att bedöma utveklingen av cyberlagstiftningen*, 16.12.2013. [http://statsradet.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=403171 / 30.6.2014]
[165] The Guardian 6.6.2013, *NSA collecting phone records of millions of Verizon customers daily*. [http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order / 18.7.2014]
[166] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 34–36.
[167] Sigholm, Johan. "Non-State Actors in Cyberspace Operations", Vankka, Jouko. (ed). *Cyber Warfare*, National Defence University, Department of Military Technology, Publication Series 1, No. 34, Helsingfors 2013, s. 50.
[168] Catharina Candolin. Intervju 7.2.2014.
[169] Kiravuo, Timo. "Offensive Cyber-capabilities against Critical Infrastructure", Vankka, Jouko. (ed). *Cyber Warfare*, National Defence University, Department of Military Technology, Publication Series 1, No. 34, Helsingfors 2013, s.78.

spelregler för att på så sätt bättre kunna skydda nationella intressen och göra cyberdomänen mera förutsebara[170].

4.1 Synen på cyberlagstiftningen i Finland och Sverige

Finland försöker med hjälp av en förnyad lagstiftning stärka sin cybersäkerhet. I den nationella cyberstrategins handlingsmodell nämner man en granskning av lagstiftningen som en huvudpunkt. Enligt den, bör lagstiftningen gynna samarbete och utvecklingen av cybersäkerheten.[171] Finland erkänner att hoten uppstår och försvinner snabbt i cyberrymden[172]. Därför anser man det vara viktigt att den behöriga myndigetens normala befogenheter bör möjliggöra omedelbart ingripande. Detta innebär även att man med hjälp av lagstiftningen måste dela upp ansvaret mellan myndigheterna och näringslivet.[173]

Kort sammanfattat, försöker Finland identifiera de hinder och begränsningar i lagstiftningen som försvårar förebyggandet, upptäckandet och avvärjandet av cyberhot. I lagstiftningsarbetet vill man beakta internationella förpliktelser och i utvecklandet av lagstiftningen betonar man internationellt samarbete. Man bedömer att de viktigaste punkterna, som måste ingå i lagstiftningen, är riktlinjer för insamling, hantering, överlåtelse och utbyte av information.[174] Försvarsminister Carl Haglund betonar att detta måste ske så att den enskilda medborgarens integritetsskydd och rätt till yttrandefrihet inte hotas[175].

Finland har ännu inte någon enhetlig lagstiftning för cyberdomän, men man har börjat kartlägga hur lagstiftningen kan utvecklas, tillsammans med förvaltningsområdena och näringslivet. Målet med kartläggningen är att ge tillräckliga möjligheter och rättigheter åt myndigheterna att ingripa och försvara nationella intressen mot eventuella cyberhot. Enligt Finland bör val av juridiskt regelverk bero på hotets ursprung och syfte.[176] Antti Pirinen är på samma linje och beskriver att man först måste definiera hoten som man vill avvärja, innan man väljer metoderna[177].

---

[170] Kamal, Ahmad. *The Law of Cyber-Space: an invitation to the table of negotiations*, United Nations, Institute of Training and Research, New York 2005, s. 3.
[171] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 5.
[172] Ibid. s. 19.
[173] Ibid. s. 35–36.
[174] Ibid.
[175] Haglund, Carl. *Ukraina i kris*, försvarsminister Carl Haglunds kolumn , Finlands försvarsministerium 14.12.1013. [http://www.defmin.fi/?l=sv&s=688 / 30.6.2014]
[176] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 10–33.
[177] Antti Pirinen. Intervju 11.7.2014.

Juridiskt sett delar Finland in cyberhoten i fyra olika kategorier: 1) enskild straffrättslig gärning, 2) ett vidsträckt terroristbrott, 3) en diplomatisk konflikt och 4) en militär konflikt. Som handlingsförfaranden i dessa olika fall, nämner man kapitel 34 i strafflagen, territorialövervakningslagen, beredskapslagen, lagen om försvarstillstånd, lagen om försvarsmakten samt kommunikationslagen och lagen om dataskydd vid elektronisk kommunikation. [178] Alla dessa lagar måste överses, då man förbereder en ny lagstiftning. Därtill måste också grundlagen överses ifall lagförändringarna påverkar medborgarnas grundläggande rättigheter[179].

Den 13 december 2013 tillsatte försvarsminister Carl Haglund en arbetsgrupp för att bedöma hur den nationella lagstiftningen borde utvecklas, så att Finland skall kunna sörja för cybersäkerheten som en del av den nationella säkerheten[180]. Den 14 mars 2015 presenterade arbetsgruppen sitt betänkande[181]. I betänkandet står det att det är ett allvarligt säkerhetshot att Finland inte har någon författningsgrund för underrättelseverksamhet i cyberrymden. Arbetsgruppen föreslår att det bör övervägas om försvarsmakten och Skyddspolisen kunde få befogenheter för underrättelse av nättrafik som kommer utomlands ifrån.[182] Utifrån sett påminner detta om de befogenheter som Sverige gett Försvarets radioanstalt i och med *Lag* (2008:717) *om signalspaning i förunderrättelseverksamhet*[183]. I Sverige har lagen fått det informella namnet ”FRA-lagen”.

Försvarsministeriets arbetsgrupp nämner att det vore ändamålsenligt att koncentrera ansvaret till en myndighet[184]. I Finland är polisväsendet för tillfället den ledande förutredningsmyndigheten för cyberbrott. Målet är att polisen skall ha förmåga att förebygga, upptäcka och avvärja cyberhot. Därför är det viktigt att utveckla sådana befogenheter som berör underrättelse och undersökning.[185] För övrigt är linjen den att försvarsmakten endast utvecklar sådan kapacitet som stöder dess lagstadgade uppgifter och att dessa förmågor vid behov kan användas som handräckning åt andra myndigheter.[186]

---

[178] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 34–35.
[179] Finlands försvarsministerium, *Riktlinjer för en finsk underrättelselagstiftning*. Betänkande av arbetsguppen för en informationsanskaffningslag 14.1.2015, Helsingfors 2015, s. 3.
[180] Finlands försvarsministerium, *Arbetsgrupp tillsatt för att bedöma utvecklingen av cyberlagstiftningen*, 13.12.2013.
[http://www.defmin.fi/sv/uppgifter_och_verksamhet/lagstiftning/lagberedning/arbetsgrupper/arbetsgrupp_tillsatt_for_att_bedoma_utvecklingen_av_cyberlagstiftningen / 5.3.2015]
[181] YLE nyheter 14.1.2015, *Försvarsmakten och Skypo föreslås få spana på nätet*.
[http://svenska.yle.fi/artikel/2015/01/14/forsvarsmakten-och-skypo-foreslas-fa-spana-pa-natet / 5.3.2015]
[182] Finlands försvarsministerium (2015) *Riktlinjer för en finsk underrättelselagstiftning*, s. 3.
[183] Sveriges försvarsdepartement, *Lag om signalspaning i försvarsunderrättelseverksamhet*, lag (2008:717), Stockholm 2008.
[184] Finlands försvarsministerium (2015) *Riktlinjer för en finsk underrättelselagstiftning*, s. 3.
[185] Ibid.
[186] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 9.

Finlands mål för underrättelseverksamheten skulle vara att skaffa information om personer och informationssystem, för att på så sätt stöda högsta statsledningens beslutsfattning. Enligt betänkandet är det viktigt att besluten grundar sig på ”*korrekt, aktuell och tillförlitlig*” information. Med den nya underrättelselagen skulle man samtidigt ge myndigheterna nya möjligheter att proaktivt avvärja cyberhoten. Enligt betänkandet bör styr- och ansvarsförhållandena bedömas genom fortsatt beredning. Arbetsgruppen konstaterar att de föreslagna förändringarna skulle vara så stora att de krävde en grundlagsförändring.[187]

Betänkandet är ett konkret exempel på målen för Finlands säkerhetisering. Diskussionen som uppstått kring betänkandet är också typiskt för säkerhetisering. Bland annat trafik- och kommunikationsministeriet lämnade in en avvikande åsikt[188]. Ministeriet påstår att arbetsgruppen från första början tillsattes för att motivera nätövervakning. Enligt dem får det inte vara en automation att Finland utför aktiv nätspaning, fastän andra länder skulle göra det.[189] Enligt trafik- och kommunikationsminister Krista Kiuru är det som om man skulle tillåta allmän husrannsakan[190]. Skyddspolisens chef Antti Pelttari ser igen på detta genom de lagstadgade uppgifter som skyddspolisen har i Finland. Enligt honom skulle en lagändring vara nödvändig för att Skyddspolisen skall kunna utföra sina lagstadgade uppgifter i cyberdomänen.[191]

Sverige utgår också ifrån att cyberattacker i första hand utreds som misstänkta brott av polismyndigheter, inom ramen för deras mandat och befogenheter.[192] Sverige påpekar att det är statens uppgift att se till att det inte sker otillåtna kontroller eller övervakning av medborgarna, och att den personliga integriteten skyddas enligt den gällande lagstiftningen. Genom att betona anonymitet och bevakning av den personliga integriteten, kan staten värna om medborgarnas förtroende för it och Internet. Sverige uttrycker att samma värderingar, fastslagna principer och lagar borde så väl on-line som off-line. Detta också då det kommer till statens rätt att utföra övervakning och underrättelse.[193]

---

[187] Finlands försvarsministerium (2015) *Riktlinjer för en finsk underrättelselagstiftning*, s. 3.
[188] Helsingin Sanomat 11.1.2015, *Työryhmä ehdottaa armeijalle ja poliisille lupaa verkkotiedusteluun - viestintäministeriö vastustaa kiivaasti*. [https://www.hs.fi/kotimaa/a1420864745560 / 5.3.2015]
[189] Helsingin Sanomat 11.1.2015, *Työryhmä ehdottaa armeijalle ja poliisille lupaa verkkotiedusteluun - viestintäministeriö vastustaa kiivaasti*. [https://www.hs.fi/kotimaa/a1420864745560 / 5.3.2015]
[190] Kaleva 12.1.2015, *Kiuru verkkovalvontamietinnössä: Kuin sallisi kotietsinnän joka kotiin*. [http://www.kaleva.fi/uutiset/kotimaa/kiuru-verkkovalvontamietinnosta-kuin-sallisi-kotietsinnan-joka-kotiin/686451/ / 12.1.2015]
[191] YLE nyheter 29.11.2014, *Supo: Suomessa yhtä paljon vakoojia kuin kylmän sodan aikana*. [http://yle.fi/uutiset/supo_suomessa_yhta_paljon_vakoojia_kuin_kylman_sodan_aikana/7659743 / 5.3.2015]
[192] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 37–38.
[193] Sveriges näringsdepartement (2011) *It i människans tjänst – en digital agenda för Sverige*, s. 14–15.

Sveriges Försvarshögskolas rapport påpekar att den nödvändiga lagstiftningen redan existerar i Sverige. Försvarshögskolan säger att det handlar om att göra medvetna tolkningar på befintliga regelverk.[194] Detta visar att Sverige ser mycket olika på lagstiftningen. Rapporten påstår att det som fattas är ett sammanhållet system av regleringar och en helhetsyn på vad man kan åstadkomma med den befintliga lagstiftningen[195].

Man kan gott säga att cyberdomänet har skapat en gråzon mellan den interna och externa säkerheten, som inte tidigare har existerat. Denna gråzon gör det svårt för myndigheter att tillämpa entydiga regelverk vid förebyggande, utredande och avvärjande av cyberattacker. Försvarshögskolans rapport har gjort ett försök att definiera gråzonen inom cyberområdet, som lagstiftningen måste ta ställning till. Enligt rapporten måste man definiera när cyberattacker skall tolkas som vanliga brott och när de skall tolkas som attacker mot den nationella säkerheten. Viktigast i detta fall är att lagstiftningen drar gränsen mellan olika myndigheters mandat och befogenheter.[196]

Som ett exempel på en gråzon nämner Finland cyberterrorismen[197]. I den nationella cybersäkerhetsstrategin, nämns polisen som ansvarismyndighet i dessa fall[198]. Sverige anser utöver detta att förebyggandet och hanteringen av cyberterrorism kräver ett nära samarbete mellan polis och militär. Därför har Sverige genom lagen (2006:343) och förordningen (2006:344) om *Försvarsmaktens stöd till polisen vid terrorismbekämpning* redan gett Försvarsmakten och polisen rätten att samarbeta[199]. Det som fortfarande försvårar bekämpningen av cyberterrorism, är att man ännu inte har någon juridisk definition på vad som är cyberterrorism.[200]

Sverige lyfter fram handlingsregler som en lösning på hur myndigheterna får och skall agera. Handlingsreglerna är inte det samma som regelverk, utan det är en implementering av gällande lagstiftning som ger ramar och riktlinjer för hur polisen skall gå till väga i olika situationer. Rapporten bedömer att man på detta sätt kan ge polisen ett effektivt instrument för att kunna agera proaktivt vid förhindrandet och utredandet av misstänkta brott i cyberrymden. Handlingsreglerna är, på samma sätt som lagstiftningen, en balansgång mellan att ge myndigheterna tillräckligt starka medel för att kunna agera och personlig integritet. Det är viktigt att

[194] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 35–41
[195] Ibid.
[196] Ibid.
[197] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 19.
[198] Ibid. s. 27.
[199] Sveriges justitiedepartement, *Försvarsmaktens stöd till polisen vid terrorismbekämpning*, lag (2006:343), Stockholm 2008.
[200] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 41.

kriminaliseringen av brottsligt beteendet på nätet är i takt med motsvarigheterna i den fysiska världen. Sverige är av den åsikten att det vore bra att utveckla handlingsreglerna gemensamt mellan länder, så att de fastställer en gemensam syn på åtgärder mot cyberbrott, för att på så sätt effektivera hanteringen av dem.[201]

Finland anser att de internationella reglerna och lagarna har en stor betydelse då man utformar sina nationella lagar. Därför vill man understryka internationellt samarbete vid utvecklandet av lagstiftningen. I det internationella arbetet vill man betona öppet informationsutbyte, gemensamma juridiska regelverk, samt överenskommen ansvarsfördelning mellan olika aktörer. Det är dock viktigt att man beaktar den internationella lagstiftningen och EU-lagstiftningen, som redan hänför sig till cyberhot.[202] Cybersäkerhetsstrategin nämner att man måste beakta den internationella lagstiftningen vid informationsbehandling och överlåtelse av information mellan olika myndigheter. Samtidigt nämner den att man med lagstiftning måste bestämma hur insamling och hantering av information skall ske så att medborgarmas integritetsskydd inte hotas.[203]

Finland anser att ett problem är att det ännu inte finns något enhetligt internationellt fördrag[204]. Sverige anser att detta går att lösa genom att svara på frågan: vad kan man reglera nationellt och vad kräver internationella överenskommelser[205]. Eneken Tikk-Ringas har disputerat inom ämnet ”rättslig strategi för cybersäkerhet” och är av den åsikten att man inte endast blint får stirra på den internationella lagstiftningen, eftersom den ofta är rätt generell. Enligt henne finns det inga garantier på att det internationella samarbetet når den nödvändiga nivån av konsensus. Därför bör den internationella lagstiftningen, enligt henne, endast uppfattas som en allmän riktlinje.[206]

Sverige erkänner att olika länders syn på mäskliga rättigheter, samt förebyggande och utredning av kriminella brott internationellt sett är stötestenar[207]. Enligt Finland har det internationella samfundet har tillsvidare inte lyckats enas om maktmedel eller sanktioner mot länder som utför cyberattacker, eftersom de entydigt inte kan tolkas som väpnade attacker[208]. För-

[201] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 38–39.
[202] Ibid. s. 35.
[203] Ibid. s. 10.
[204] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 34.
[205] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 35–36.
[206] Tikk-Ringas, Eneken. “Cyber Security: Solutions of Tomorrow, Experience of Yesterday”, Huldt, Bo & Sivonen, Pekka & Ries, Tomas & Huldt, Camilla. (ed) *Strategic Yearbook 2012-2013. The Emerging Global Security Environment*, Edita Västra Aros, Västerås 2013, s. 180–182.
[207] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 36–40.
[208] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 34.

svarshögskolans rapport uttrycker att en internationell lagstiftning därför är nödvändig i frågor gällande utförandet av cyberoperationer som en del av konventionell krigsföring, eller vid utförandet av sanktioner som nämns i artikel 41 och 42 i FN-stadgan[209].[210] I Sverige pågår det som bäst diskussioner om hur man borde definiera cyberattacker i förhållande till traditionell konventionell krigsföring.[211] Catharina Candolin säger att man kunde jämföra cyberattacker med kränkning av luftrum[212]. Jarno Limnéll säger ändå att cyberattacker ofta är allvarligare, eftersom den åstadkommer konkret fysisk eller ekonomisk skada[213].

Enligt Försvarshögskolans rapport är ett av de största problemen ändå att man inte har gemensamma, juridiskt klassificerade, definitioner inom cyberdomänet. Om det skulle finnas en sammanhållen juridisk definition, skulle det vara lättare att enas om motåtgärder.[214] Denna undersökning föreslår som en lösning att man först borde definiera cyberterminologin nationellt och sedan formar om den efter internationella överenskommelser.

Det är värt att notera att Sveriges digitala agenda talar om att friheten och säkerheten på nätet hör till de stora globala framtidsfrågorna. Sverige anser att ärendet påverkar grundläggande frågor såsom frihet, mänskliga rättigheter, yttrande- och åsiktsfrihet samt demokratisering.[215] Ur Sveriges digitala agenda framgår det att målet med lagstiftningen borde vara att stärka de positiva möjligheterna som it-omgivningen medför och minimera de negativa effekterna, som till exempel brottslighet på nätet.[216] Som brottsliga handlingar nämns informationsläckage, lösenordsfiske och bedrägeri.[217]

För att uppfylla EU:s direktiv om *angrepp mot nationella informationssystem*[218], har Sveriges regering överlämnat en remiss till Lagrådet för *skärpt straff för dataintrång*. Lagrådsremissen föreslår att grovt dataintrång borde bestraffas med minst 6 månaders och högst 6 års fängelse. Regeringen föreslår samtidigt att också försök och förberedelse av grovt dataintrång bör be-

---

[209] Artikel 41 och 42 i FN-stadgan talat om Säkerhetsrådets rätt att besluta om sanktioner och åtgärder, då den internationella säkerheten hotas. Se: Förenta Nationerna, *Förenta Nationernas stadga och stadga för den internationella domstolen*, 1945. [http://www.fn.se/PageFiles/1158/FN-stadgan.pdf / 17.3.2014], s. 9.
[210] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 36–40.
[211] Sigholm, J. (2013) "Non-State Actors in Cyberspace Operations", s. 52.
[212] Catharina Candolin. Intervju 7.2.2014.
[213] Jarno Limnéll. Intervju 7.4.2014.
[214] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 41.
[215] Sveriges näringsdepartement (2011) *It i människans tjänst – en digital agenda för Sverige*, s. 53.
[216] Ibid.
[217] Ibid.
[218] Europaparlamentet, Europaparlamentets lagstiftningsresolution 2010/0273(COD), 4.7.2013. [http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0321&language=SV&ring=A7-2013-0224 / 1.7.2014]

straffas.[219] Finlands justitieministerium har tillsatt en arbetsgrupp för att ratificera samma direktiv[220].

Vidare upplever Sverige att privata företag, och framför allt internationella företag, utgör en utmaning för den nationella lagstiftningen. Nätverken är beroende av företag, som fysiskt administreras utomlands ifrån. Lagstiftningen måste ge svar på hur man effektivt kan hantera och kontrollera dessa företag, utan att dessa upplever att regleringen är för stor. I andra fall kan det leda till att företagen flyttar sin verksamhet till länder, där de upplever att regleringen är liten.[221] Finland är inne på samma linje då man anser att man kan gynna ekonomin med hjälp av en enhetlig lagstiftning. Enligt Finland är det lättare att locka företag och utländska investeringar om dessa upplever att nätverken och cybersäkerheten stöder deras verksamhet.[222]

4.2 Försvarets radioanstalt som berättigad säkerhetsaktör

Sverige har lyckats bygga upp en fungerande och effektiv övervakning och underrättelse i cyberrymden, med hjälp av de befogenheter som getts åt Försvarets radioanstalt (FRA) i lagen (2008:717) *om signalspaning i förunderrättelseverksamhet*.[223] Lagen ger Försvarets radioanstalt rätten att övervaka och utföra signalspaning av kabelburen trafik, som passerar Sveriges gränser. [224] Lagen är inte endast till för att främja cybersäkerheten, utan den omfattar också andra säkerhetspolitiska mål. De säkerhetspolitiska målen med lagen är att:

- reda ut militärförmåga hos främmande länder
- stöda Sveriges militära insatser utomlands
- hindra utveckling och spridning av massförstörelsevapen
- bekämpa internationell terrorism
- försvara Sverige mot it-angrepp från utlandet, som är riktade mot känsliga informationssystem

---

[219] Sveriges regering, *Lagrådsremiss – Skärpt straff för dataintrång*. Regeringens remiss till Lagrådet 16.1.2014, Stockholm 2014, s. 1.
[220] Säkerhetskommittén (2014) *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*, s. 4.
[221] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 36.
[222] Finlands försvarsministerium (2013) *Strategi för cybersäkerheten i Finland*, s. 1.
[223] Pehrson Johan. *FRA och signalspaning*, debattartikel, Folkpartiet 6.4.2007. [https://www.folkpartiet.se/politiker/ledamoter-av-riksdagen/johan-pehrson/debattartiklar/fra-och-signalspaning/ / 3.7.2014]
[224] Sveriges försvarsdepartement, *Lag om signalspaning i försvarsunderrättelseverksamhet*, lag (2008:717), Stockholm 2008.

- försvara mänskliga rättigheter i auktoritärt styrda länder[225]

Detta har samtidigt resulterat i en centraliserad övervakningsmodell[226]. Övervakningsmodellen är ännu idag omstridd bland politiker och medborgare[227], men den har också gett resultat. Enligt Säkerhetspolisens operativa chef Anders Kassman har Säkerhetspolisen lyckats hindra två terrordåd tack vare FRAs signalspaning[228].

Sverige motiverade FRA-lagen med hjälp av åtgärder som uppfyller definitionen på säkerhetisering. De tydligaste elementen var förknippade med en talesakt och den debatt som pågick mellan lagförslagets anhängare och motståndare.[229] Flera samhällsaktiva påstod att lagen är ett intrång på integriteten och att det finns en stor risk för missbruk av information.[230] Regeringen var tvungen, på grund av det hårda politiska och medborgerliga motståndet, att göra ändringar i det ursprungliga lagförslaget. Den omdebatterade lagen godkänndes 4 år efter att det första lagförslaget hade getts ut.[231]

Det är ändå svårt att säga om FRA:s roll i framtiden kommer att ändra. Johan Sigholm säger att FRA-lagen fortfarande har motståndare och att detta, i framtiden, kan led till en kamp om myndigheternas roll och resurser.[232] Detta skulle dock kräva en stor förändring i Sveriges cybersäkerhetspolitik.

---

[225] Försvarets radioanstalt (FRA), *Verksamhet*, [http://www.fra.se/verksamhet.4.html / 26.2.2014]
[226] Antti Pirinen. Intervju 11.7.2014.
[227] SVT, Uppdrag granskning, 11.12.2013. [http://www.youtube.com/watch?v=t8OI0aPzVH8 / 19.1.2014]
[228] SvD nyheter 3.9.2014, *Säpo hindrade två terrordåd*. [www.svd.se/nyheter/inrikes/sapo-stoppade-terrordad_3877326.svd?sidan=1 / 5.3.2015]
[229] SVT, Uppdrag granskning, 11.12.2013. [http://www.youtube.com/watch?v=t8OI0aPzVH8 / 19.1.2014]
[230] Linder, P.J. Anders. *Riksdagen måste säga nej till Lex Orwell*, ledare, Svenska Dagbladet 9.3.2007. [http://www.svd.se/opinion/ledarsidan/riksdagen-maste-saga-nej-till-lex-orwell_1069817.svd / 3.3.2014]
[231] Brandberg, Ulrika. *FRA-lag godkänd trots kritik*, Advokaten, nummer 8 2009 årgång 75. [https://www.advokatsamfundet.se/Documents/Advokaten/low_Advokaten%202009-8.pdf / 26.2.2014]
[232] Sigholm, Johan. Brevväxling 1.2.2014.

5 IMPLIKATIONER

Denna undersökning har analyserat Finlands och Sveriges cybersäkerhetspolitik genom den säkerhetisering som länderna utför. Resultaten visar att det både finns likheter och olikheter i ländernas cybersäkerhetspolitik. Bilaga 1, presenterar en sammanfattning på detta.

Den största likheten är att länderna har valt att behandla cybersäkerheten utan att avskilja den från den övriga säkerheten. Detta är en fortsättning på *totalförsvarstänkandet*[233] som starkt styr bägge ländernas säkerhetspolitik. Utförd analys visar ändå att detta sker på olika sätt i Finland och i Sverige.

Finland har förankrat cybersäkerheten till den nationella cybersäkerhetsstrategin, medan Sverige har tagit cybersäkerheten med i säkerhetspolitiken under begreppet informationssäkerhet. Finlands säkerhetisering har också under de senaste åren varit synligare, vilket har lett till att cybersäkerheten fått en större betydelse i den finska säkerhetspolitiska diskussionen.

En orsak till skillnaden är att Sverige redan säkrat sin statliga närvaro i cyberrymden med hjälp av den omtalade FRA-lagen. De svenska beslutsfattarna har därför upplevt sig tillsvidare kunna uppfölja de nationella säkerhetsintressena med befintliga medel. Detta har också lett till att Sverige inte har haft behov av en separat cybersäkerhetsstrategi.

En annan orsak till den synliga skillnaden mellan Finlands och Sveriges cybersäkerhetspolitik är ländernas sätt att definiera begreppet ”informationssäkerhet”. I finskan kan ordet syfta både på ”tietoturva” eller ”tietoturvallisuus”, medan svenska ordet ”informationssäkerhet” omfattar båda begreppen.[234] Det är en orsak som förklarar varför Sverige har valt behandla cybersäkerheten under begreppet informationssäkerhet. Sveriges Försvarshögskola anser att cybersäkerhet är ett horisontellt begrepp som fokuserar på nätverk, medan informationssäkerhet igen behandlar den vertikala dimensionen, som till exempel folkrättsliga frågor[235].

---

[233] Jämför: sv. *totalförvar* [http://www.sakerhetspolitik.se/Sakerhetspolitik/Svensk-sakerhet/Totalforsvar/] och fi. *kokonaismaanpuolustus* [http://www.defmin.fi/tehtavat_ja_toiminta/kokonaismaanpuolustus].

[234] Antti Pirinens (intervju 11.7.2014) åsikt är att detta är ett allmänt godtaget förfarande och att en cybersäkerhetsstrategi ofta påminner om en informationssäkerhetstrategi. Jämför med fin. ”tietoturvallisuus”. Limnéll, J., Majewski K. & Salminen M. (2014) *Kyberturvallisuus*, s. 55–56, är av den åsikten att cybersäkerheten är ett mycket bredare begrepp än informationssäkerhet. Jämför med fin. ”tietoturva”. Antti Pirinen poängterar här att man måste skilja på orden ”tietoturva” och ”tietoturvallisuus”. Detta leder till en betydande skillnad, då det svenska ordet ”informationssäkerhet” omfattar båda två. Genom detta uppstår en frågeställning om detta kan vara en orsak till att Sverige har valt att behandla cybersäkerhet inom ramen för informationssäkerhet?

[235] Sveriges Försvarshögskola (2012) *Rapport Cyberförsvar*, s. 3.

Finlands fördel, jämfört med Sverige, är att man redan kommit relativt långt med ett målmedvetet strategiskt arbete. Enligt denna analys är Finlands slutliga mål för säkerhetiseringen att satsa nya resurser på cybersäkerheten och att ge myndigheterna större befogenheter genom en uppdaterad lagstiftning.

Finlands nationella cybersäkerhetsstrategi har också kommit med konkreta förslag på hur det skall ske. Enligt Jarno Limnéll kräver denna implementering tre saker: 1) att man frigör tillräckligt mycket ekonomiska resurser, 2) att man uppdaterar lagstiftningen och 3) att ledningen centraliseras. På lång sikt har det finska strategiarbetet goda möjligheter att resultera i fungerande cybersäkerhetsmodeller. [236]

Jyrki Kasvi har dock kritiserat den planerade dimensioneringen av resurser till att vara för liten[237]. Catharina Candolin säger igen att Finlands nationella cybersäkerhetsstrategi är en kompromiss och att den därför inte tillräckligt entydigt definierar myndigheternas ansvarsuppdelning. En annan svaghet är att den inte beskriver någon klar vision för hur processen för den framtida övervakningen borde se ut. Den tar inte heller näringslivet i beaktande i en tillräckligt stor utsträckning.[238]

Gemensamt för Finland och Sverige, när det kommer till lagstiftningen, är att båda betonar medborgarnas grundläggande friheter och rättigheter, något som nämns i både Finlands grundlag och Sveriges regeringsform. Respektive land anser att många av lagstiftningsfrågorna måste lösas på ett internationellt plan. Som Sverige nämner, utesluter detta inte att man redan nu kunde ändra på lagstiftningen och skapa juridiska definitioner också på en nationell nivå. Denna undersökning föreslår därmed att de juridiska definitionerna först kunde fastställas nationellt och sedan ersättas, då de internationella motsvarigheterna träder i kraft.

Denna undersökning visar att Sverige de facto har beaktat lagstiftningen på en bredare front. Flera av dokumenten hänvisar till själva paragraferna, samtidigt som de framför konkreta förbättringsförslag. Sverige har hittills intagit flera juridiska ståndpunkter än Finland. Nämnvärda ståndpunkter är synen på: myndigheternas närvaro, straff för dataintrång och bekämpning av cyberterrorism.

---

[236] Jarno Limnéll. Intervju 7.4.2014.
[237] Iltalehti 26.1.2013, *Kasvi lyttää: Kyberturvallisuusstrategia on vitsi*. [http://www.iltalehti.fi/uutiset/2013012616603425_uu.shtml / 4.7.2014]
[238] Catharina Candolin. Intervju 7.2.2014.

Den största skillnaden är ändå att Sverige inte har något större behov att stifta nya lagar. Sverige anser att de endast måste besluta hur den redan existerande lagstiftningen skall tillämpas på cyberdomänet. Finland har i detta fall valt en annan linje. Utförd analys visar att Finlands mål är att författa en helt ny lagstiftning för cyberdomänet.

Både Finland och Sverige understryker ett starkt myndighetssamarbete, vilket kan ses som en bra sak. Samarbete myndigheterna emellan ligger emellertid i en gråzon, där befogenheterna juridiskt måste fastställas. Analysen visar att båda anser att huvudansvaret borde ges åt en enda myndighet. Både Finland och Sverige föreslår att det skulle vara polisen. Sverige har dock lyckats definiera en tydligare struktur för myndighetssamarbete än Finland. Utöver detta har Sverige nämnt handlingsreglerna som en metod för att effektivera och förenkla myndigheternas arbete.

Finland och Sverige erkänner att lägesbilden är viktig för att cyberhoten skall kunna avvärjas. Detta innebär en mängd ekonomiska satsningar[239]. Det är ändå praktiskt taget omöjligt att skapa en fullständig lägesbild, oberoende av resursernas storlek. Man måste därför, med hjälp av noggrannare utredningar, avgöra hur stor osäkerhet som går att godkänna i förhållande till satsningarna.[240] Skapandet av lägesbilden är dock en utmaning om myndigheterna inte har befogenheter att utföra aktiv nätspaning av datatrafik. Sverige har på denna front en bättre förmåga att skapa och upprätthålla en lägesbild i realtid tack vare de befogenheter som getts åt FRA.

Antti Pirinen förklarar att en aktiv nätspaning skulle kräva mera ekonomiska resurser än de som Finland för tillfället använder på cybersäkerhet[241]. En passiv modell har den fördelen, att den med stor sannolikhet skapar ett större förtroende bland medborgarna. Han är av den åsikten att företagen själv klarar av att skydda sina nätverk och att de i första hand förväntar sig transparens och förutsägbarhet av myndigheterna. Därför kan en väl fungerande passiv nätspaningsmodell i bästa fall skapa mera förtroende i företagens ögon, än en dåligt fungerande aktiv modell.[242]

Ifall Finland i framtiden väljer att endast bygga sitt cyberförsvar på passiva metoder, kommer den totala förmågan att övervaka cyberrymden att vara något sämre än Sveriges. Antti Pirinen

[239] Catharina Candolin. Intervju 7.2.2014.
[240] Limnéll, Jarno. ”Cybersäkerhet, en strategisk utmaning”, tal på konferensen för säkerhets- och informationssystem i Monaco 8.10.2013. [https://www.youtube.com/watch?v=qzmHc3guvjw / 4.7.2014]
[241] Antti Pirinen. Intervju 11.7.2014.
[242] Ibid.

säger att en nationell cybersäkerhetsstrategi i först hand skall säkra och skydda de nationella säkerhetsintressena[243]. Han är ändå av den åsikten att det handlar om en balansgång mellan användning av resurser och de hot man vill avvärja. Enligt honom kunde den nuvarande finska modellen, tillsammans med ett utökat internationellt samarbete, mycket väl kunna räcka till, för att skydda de egna systemen och den sekretessbelagda informationen. Viktigaste är att övervakningen är centraliserad och att ansvarsmyndigheten har rätt att handla omedelbart. Det är en annan sak om Finland till exempel vill kunna upptäcka och utreda brott så som i den fysiska världen eller om Finland vill kunna utreda brott som inte är riktade mot de statliga nätverken. I så fall krävs införandet av en aktiv nätspaning.[244]

Jarno Limnéll säger att övervakningsmekanismerna måste vara i skick om Finland tänker gå in för en aktiv nätspaning. I andra fall riskerar man att skrämma bort företag.[245] Antti Pirinen säger att det sist och slutligen handlar om att hitta en modell som passar Finlands säkerhetskultur och syn på demokrati.[246]

Försvarsminister Carl Haglund säger i en intervju för Rundradion att en parlamentarisk övervakning är ett alternativ för att skydda medborgarnas integritet, ifall Finland väljer att gå in för en aktiv spaning av cyberrymden[247]. Chefen för EU:s underrättelseanalyscentrum (Intcen), Ilkka Salmi, säger i A-studions intervju för Rundradion att han upplever att parlamentarisk övervakning innebär att beslutsfattarna bestämmer vad som bör övervakas och att myndigheterna redogör för vad som har övervakats. Även han upplever att myndigheterna borde ha möjlighet till aktiv nätspaning i ärenden som berör deras egna verksamhetsområden: Försvarsmakten inom det militära, polisen vid utredningen av brott och Skyddspolisen i ärenden som berör statshemlighet och -säkerhet.[248] Utförd analys visar att det inte endast räcker med en parlamentarisk övervakning, utan att det också måste finnas fastställda regelverk för överlåtelse av information mellan myndigheterna.

Det finns också andra som anser att myndigheterna bör utföra aktiv nätspaning. Detta är förståeligt, då man tänker på de brott och hotbilder som dessa organisationer jobbar med. I en in-

[243] Antti Pirinen. Intervju 11.7.2014.
[244] Ibid.
[245] Jarno Limnéll. Intervju 7.4.2014.
[246] Ibid.
[247] YLE nyheter 18.11.2013, *Staten ska inte övervaka din Facebook*. [http://svenska.yle.fi/artikel/2013/11/08/staten-ska-inte-overvaka-din-facebook / 4.7.2014]
[248] YLE, A-studio 17.3.2014, program 10/637. Myndigheterna har redan en del befogenheter att utföra underrättelse inom sitt eget verksamhetsområde. Det som nu diskuteras är till vilken utsträckning som befogenheterna borde utvidgas att gälla cyberdomänet.

tervju för Talouselämä säger Skyddspolisens chef, Antti Pelttari, att Finland borde ge myndigheterna befogenheter att utföra underrättelseverksamhet i cyberrymden[249]. Också polisöverdirektör Mikko Paatero har krävt mera befogenheter åt polisen[250]. Han är också av den åsikten att polisen och Försvarsmakten kunde ha gemensamma resurser då det kommer till bekämpningen av cyberterrorism[251].

En eventuell lagstiftningsförändring innebär att man måste väga mellan de nationella säkerhetsintressena och medborgarnas personliga integritet. Carl Haglund sade i sitt tal på den 207:e Försvarskursen att man då måste beakta hur mycket medborgarna är villiga att lita på myndigheterna[252]. Ilkka Salmi ser ingen motsättning mellan de nationella säkerhetsaktörerna och medborgarna[253]. Han säger ändå att det är en betydande samhällsfråga, där alla måste få uttrycka sig[254]. Slutresultatet kommer till en stor del att bero på hur Finlands säkerhetisering lyckas.

[249] Talouselämä 20.6.2013, *Supo haluaa seurata sinua tarkemmin verkossa*.
[http://www.talouselama.fi/uutiset/supo+haluaa+seurata+sinua+tarkemmin+verkossa/a2191293 / 3.7.2014]
[250] Helsinki Times 8.11.2013, *Paatero: Police wants authority to monitor Internet traffic*.
[http://www.helsinkitimes.fi/finland/finland-news/domestic/8331-paatero-police-wants-authority-to-monitor-internet-traffic.html / 3.7.2014]
[251] Ibid.
[252] Haglund, Carl. *Puolustusministeri Carl Haglundin puhe 207. Maanpuolustuskurssin avajaisissa*, Finlands försvarsministerium 11.11.2013.
[http://www.defmin.fi/ajankohtaista/puheet/puolustusministeri_carl_haglundin_puhe_207._maanpuolustuskurssin_avajaisissa.5655.news?661_o=10 / 4.7.2014]
[253] YLE, A-studio 17.3.2014, program 10/637.
[254] Ibid.

6 DISKUSSION

Arbetet lyckades svara på forskningsfrågorna genom att applicera forskningsmetoden på de statliga dokumenten. Intervjuerna stödde analysen, samt gav nya och intressanta synpunkter på cybersäkerhetsfrågor. Detta möjliggjorde konkreta slutsatser. Den observationsbaserade analysens svaghet är dock att den endast fokuserar på en handfull observationer. En annan nackdel med analysmetoden är att det ibland kan vara svårt att urskilja de kausala faktorerna till ett observerat fenomenen, därför att den inte tar i beaktande historiska händelser. Det som står klart är att det har en stor skillnad vilken nivå (strategisk, operativ, teknisk) som väljs vid analys av cybersäkerhet. Om denna undersökning skulle ha valt en annan nivå så skulle svaren på forskningsfrågorna troligen sett annorlunda ut.

Säkerhetiseringsteorierna visade sig vara en lämplig referensram för analyserandet av Finlands och Sveriges cybersäkerhetspolitik. Undersökningen visar att det både Finland och Sverige genomgår en politisk process som kan tolkas som säkerhetisering. Det första tydliga tecknet är den förda samhällspolitiska debatten och det andra, det lagstiftningsarbete som Sverige redan utfört och det lagstiftningsarbete som för tillfället pågår i Finland. Nackdelen med säkerhetiseringsteorierna är att de skapar ett perspektiv som betonar allmän samhällssäkerhet. Detta leder till att enskilda, även viktiga, säkerhetsområden får mindre uppmärksamhet. Resultaten skulle i detta avseende möjligen ha varit annorlunda om undersökningen hade valt en annan teoretisk referensram.

Lagstiftningen utgjorde en intressant tvärvetenskaplig vinkling, som samtidigt vidgade perspektivet på denna undersökning. Resultaten var positiva, då lagstiftningsanalysen lyckades identifiera både likheter och olikheter mellan Finland och Sverige. Sverige visade sig också vara ett fungerande referensland. Resultatet skulle ha varit annorlunda ifall jämförelsen gjorts med något annat land. Det som denna lagstiftningsanalys inte har beaktat är följderna av de föreslagna åtgärderna som Finland borde ta.

Som vidareundersökning föreslås utredningar på hur Finland kunde ta modell av FRA-lagen och vilka konsekvenser som de föreskrivna åtgärderna skulle ha på samhället. Därpå borde man undersöka hur cyberattacker skall tolkas i förhållande till väpnade attacker. Ytterligare vidareundersökningsmöjligheter kunde vara att undersöka på vilket sätt historiska händelser har påverkat utformandet av ländernas nuvarande säkerhetsstrukturer och hur ländernas ekonomiska situationer påverkar säkerhetiseringen.

7 SAMMANFATTNING OCH KONKLUSIONER

För att skapa lag och ordning i cyberrymden har Finland och Sverige säkerhetiserat sin cybersäkerhetspolitikska agenda. Cybersäkerheten är ett typexempel hur en säkerhetsagenda kan lyftas upp i den nationella säkerhetsdiskussionen med hjälp av säkerhetisering.

Undersökningen visar att Finland och Sverige har mycket liknande mål för sin cybersäkerhetspolitik, även om det förefaller som om länderna skulle ha olika agendan. Detta beror på att länderna har valt olika strategier för säkerhetiseringen, då de försöker nå sina politiska mål. Finland vill bygga upp en ny säkerhetsstruktur, vilket innebär en intensivare och mera målmedveten säkerhetisering. Sverige vill igen stärka och förtydliga de strukturer som redan existerar och har därför valt en moderatare politisk linje för sin säkerhetisering.

Orsakerna till denna skillnad beror mestadels på två saker. För det första har länderna olika lagstiftning. Sverige har redan gett Försvarets radioanstalt rätten att utföra aktiv nätspaning, medan Finland inte har någon motsvarighet. Detta har också resulterat i att säkerhetsstrukturerna har utvecklats på olika sätt i respektive land. För det andra har Sverige valt att behandla cybersäkerheten under begreppet informationssäkerhet. Vad detta beror på är svårt att säga utan mera djupgående forskning. Denna undersökning indikerar ändå att det till en del skulle bero på språkliga definitionsskillnader mellan finskan och svenskan.

Vilken cybersäkerhetspolitik som kommer att resultera i bättre säkerhet för samhället återstår att se. En avgörande sak är hur säkerhetiseringen lyckas i respektive land och hur välvilliga politikerna är att satsa ekonomiska resurser på uppbyggandet av cybersäkerheten. Gemensamt för båda länderna är att de måste definiera cyberterminologin och bestämma hur den bör tolkas straffrättsligt.

För att nå sina målsättningar måste Finland identifiera vad som är värt att skydda och vad som krävs för att skydda olika säkerhetsobjekt mot möjliga hot. Finland måste också avgöra om man tänker idka aktiv nätövervakning eller om man vill bygga cybersäkerheten på en passiv övervakningsmodell. Båda modellerna har sina för- och nackdelar och är fungerande om de implementeras på rätt sätt. Val av modell måste bero på hotbilder, tillgängliga resurser, myndigheternas tolerans för ovisshet och medborgarnas tillit till myndigheterna. En aktiv nätspaningsmodell har dock vissa fördelar med tanke på de nationella säkerhetsintressena.
För företagen och näringslivet är det viktigt att myndighetsverksamheten är transparent och förutsägbar. Med tanke på medborgarnas integritet är det viktigt att övervakningen är parla-

mentariskt kontrollerad och att det finns fastslagna regler för utbyte av information mellan myndigheterna. Det viktiga är att införa en modell som i sin helhet skapar förtroende och en känsla av säkerhet bland medborgarna, vilket generellt är en av säkerhetiseringens grundprinciper. Undersökningen visar att Finland måste skapa en säkerhetsstruktur som lämpar sig för landets egna säkerhetsintressen och medborgarnas uppfattning om demokrati. Den visar också att Finland måste vara villig att satsa mera ekonomiska resurser på cybersäkerheten än hittills oberoende av övervakningsmetod, om man vill åstadkomma några större förändringar.

Till sist är det viktigt att minnas att cybersäkerhetspolitiken också skall möjliggöra utnyttjade av de positiva möjligheter som de digitala nätverken medför. Denna undersökning visar att Sverige har lyckats ta i beaktande användarvänlighet bättre än Finland, medan Finland har sett möjligheter som ligger i utbildning och forskning av området.

KÄLLOR

Primära källor

Statliga dokument

Finlands försvarsministerium, *Strategi för cybersäkerheten i Finland*. Statsrådets principbeslut 24.1.2013, Helsingfors 2013.

Finlands försvarsministerium, *Säkerhetsstrategi för samhället*. Statsrådets principbeslut 16.12.2010, Helsingfors 2010.

Finlands säkerhets- och försvarspolitik 2009. Statsrådets redogörelse till riksdagen 5.2.2009, SRR 1/2009 rd, Helsingfors 2009.

Finlands säkerhets- och försvarspolitik 2012. Statsrådets redogörelse till riksdagen 20.12.2012, SRR 6/2012 rd, Helsingfors 2012.

Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma. Säkerhetskommittén 11.3.2014, Helsingfors 2014.

Myndigheten för samhällsskydd och beredskap, *Strategi för samhällets informationssäkerhet 2010-2015,* Stockholm 2010.

Sveriges näringsdepartement, *It i människans tjänst – en digital agenda för Sverige*. Stockholm 2011.

Sveriges Försvarshögskola, *Rapport Cyberförsvar* (254/2012), bilaga 1. Försvarshögskolans rapport till regeringen 20.12.2012, Stockholm 2012.

Övriga primära källor

Finlands försvarsministerium, *Riktlinjer för en finsk underrättelselagstiftning.* Betänkande av arbetsguppen för en informationsanskaffningslag 14.1.2015, Helsingfors 2015.

Finlands försvarsministerium, *Strategi för cybersäkerheten i Finland*, [http://www.defmin.fi/sv/publikationer/strategidokument/strategi_for_cybersakerheten_i_finland / 18.4.2014]

Finlands grundlag, lag (11.6.1999/731).

Förenta Nationerna, *Förenta Nationernas stadga och stadga för den internationella domstolen*, 1945. [http://www.fn.se/PageFiles/1158/FN-stadgan.pdf / 17.3.2014]

Försvarets radioanstalt (FRA), *Verksamhet*, [http://www.fra.se/verksamhet.4.html / 26.2.2014]

Sveriges försvarsdepartement, *Lag om signalspaning i försvarsunderrättelseverksamhet*, lag (2008:717), Stockholm 2008.

Sveriges justitiedepartement, *Försvarsmaktens stöd till polisen vid terrorismbekämpning*, lag (2006:343), Stockholm 2008.

Sveriges regering, *Lagrådsremiss – Skärpt straff för dataintrång*. Regeringens remiss till Lagrådet 16.1.2014, Stockholm 2014.

Sveriges regeringsform, lag (2002:903).

Säkerhetskommittén, *Cybersäkerhetsstrategins verkställighetsprogram*, [http://www.turvallisuuskomitea.fi/index.php/sv/kyberturvallisuusstrategia/toimeenpano-ohjelma / 24.5.2014]

Övriga källor

Brandberg, Ulrika. *FRA-lag godkänd trots kritik*, Advokaten, nummer 8 2009 årgång 75. [https://www.advokatsamfundet.se/Documents/Advokaten/low_Advokaten%202009-8.pdf / 26.2.2014]

Europaparlamentet, Europaparlamentets lagstiftningsresolution 2010/0273(COD), 4.7.2013. [http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0321&language=SV&ring=A7-2013-0224 / 1.7.2014]

Finlands försvarsministerium, *Kokonaismaanpuolustus*,
[http://www.defmin.fi/tehtavat_ja_toiminta/kokonaismaanpuolustus / 7.7.2014]

Finlands försvarsministerium, *Arbetsgrupp tillsatt för att bedöma utvecklingen av cyberlagstiftningen,* 13.12.2013.
[http://www.defmin.fi/sv/uppgifter_och_verksamhet/lagstiftning/lagberedning/arbetsgrupper/arbetsgrupp_tillsatt_for_att_bedoma_utvecklingen_av_cyberlagstiftningen / 5.3.2015]

Finlands statsråd, *Försvarsminister Haglund tillsatte en arbetsgrupp för att bedöma utvecklingen av cyberlagstiftningen*, 16.12.2013.
[http://statsradet.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=403171 / 30.6.2014]

Finlands statsråd, *Redogörelse om Finlands säkerhets- och försvarspolitik till riksdagen*, 20.12.2012. [http://vnk.fi/ajankohtaista/tiedotteet/tiedote/sv.jsp?oid=373201 / 19.5.2014]

Finlands statsråd, *Säkerhetsstrategi för samhället*, 16.12.2010.
[http://vnk.fi/toiminta/turvallisuus/YTS/sv.jsp / 19.5.2014]

Finlands utrikesministerium, *Finlands utrikesförvaltning utsatt för dataintrång*, 1.11.2013.
[http://formin.finland.fi/public/default.aspx?contentid=291720&nodeid=23&contentlan=3&culture=sv-FI / / 15.4.2014]

Försvarets radioanstalt (FRA), *Om FRA*. [http://www.fra.se/omfra.6.html / 25.3.2015]

Försvarets radioanstalt (FRA), *Signalunderrättelseverksamhet*.
[http://www.fra.se/verksamhet/signalunderrattelseverksamhet.68.html / 25.3.2015]

Haglund, Carl. *Puolustusministeri Carl Haglundin puhe 207. Maanpuolustuskurssin avajaisissa*, Finlands försvarsministerium 11.11.2013.
[http://www.defmin.fi/ajankohtaista/puheet/puolustusministeri_carl_haglundin_puhe_207._maanpuolustuskurssin_avajaisissa.5655.news?661_o=10 / 4.7.2014]

Haglund, Carl. *Ukraina i kris*, försvarsminister Carl Haglunds kolumn , Finlands försvarsministerium 14.12.1013. [http://www.defmin.fi/?l=sv&s=688 / 30.6.2014]

International Telecommunication Union (ITU), webblpats. [http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx / 24.3.2015]

Kasvi, Jyrki. *Strategia joka katosi*, blogginlägg 24.1.2013, YLE nyheter, [http://yle.fi/uutiset/jyrki_kasvi_strategia_joka_katosi/6465713 / 4.7.2014]

Koivula, Tommi. Proseminarium 7.5.2014.

Limnéll, Jarno & Majewski Klaus & Salminen Mirva. *Kyberturvallisuus*, Docendo Oy, Jyväskylä 2014.

Limnéll, Jarno. ”Cybersäkerhet, en strategisk utmaning”, tal på konferensen för säkerhets- och informationssystem i Monaco 8.10.2013. [https://www.youtube.com/watch?v=qzmHc3guvjw / 4.7.2014]

Linder, P.J. Anders. *Riksdagen måste säga nej till Lex Orwell*, ledare, Svenska Dagbladet 9.3.2007. [http://www.svd.se/opinion/ledarsidan/riksdagen-maste-saga-nej-till-lex-orwell_1069817.svd / 3.3.2014]

Myndigheten för samhällsskydd och beredskap (MSB), *Totalförsvar*, MSBs webbplats. [http://www.sakerhetspolitik.se/Sakerhetspolitik/Svensk-sakerhet/Totalforsvar/ / 7.7.2014]

Myndigheten för samhällsskydd och beredskap (MSB), webbplats. [https://www.msb.se / 24.2.2015]

Nordiska ministerrådet, webbplats. [http://www.norden.org/sv/fakta-om-norden/politik / 24.3.2015]

OECDs, webbplats. [http://www.oecd.org/about/ / 24.3.2015]

Paronen, Antti. Proseminarium 7.5.2014 & 29.1.2015

Pehrson Johan. *FRA och signalspaning*, debattartikel, Folkpartiet 6.4.2007. [https://www.folkpartiet.se/politiker/ledamoter-av-riksdagen/johan-pehrson/debattartiklar/fra-och-signalspaning/ / 3.7.2014]

Sveriges näringsdepartement, regeringskansliet 6.10.2011. [https://www.regeringen.se/sb/d/14216/a/177256 / 24.2.2015]

Sigholm, Johan. Brevväxling 1.2.2014 & 15.2.2015.

Sivonen, Pekka. Personligt samtal 27.6.2014.

Statsrådets förordning om Säkerhetskommittén, förordning (77/2013).

SVT, Uppdrag granskning, 11.12.2013. [http://www.youtube.com/watch?v=t8OI0aPzVH8 / 19.1.2014]

YLE, A-studio, 17.3.2014, program 10/637.

Intervjuer

Catharina Candolin. Intervju 7.2.2014.

Jarno Limnéll. Intervju 7.4.2014.

Antti Pirinen. Intervju 11.7.2014.

Nyheter

Aftonbladet 27.9.2008, *Operation spionlag – Så lyckades FRA få igenom signalspaningslagen*. [http://www.aftonbladet.se/nyheter/fralagen/article11602598.ab / 3.7.2014]

Helsingin Sanomat 18.1.2013, *Verkkohyökkäyksistä leimahti kiistahallituksessa*. [http://www.hs.fi/kotimaa/a1358401486659 / 18.3.2015]

Helsingin Sanomat 11.1.2015, *Työryhmä ehdottaa armeijalle ja poliisille lupaa verkkotiedusteluun - viestintäministeriö vastustaa kiivaasti*. [https://www.hs.fi/kotimaa/a1420864745560 / 5.3.2015]

Helsinki Times 8.11.2013, *Paatero: Police wants authority to monitor Internet traffic*. [http://www.helsinkitimes.fi/finland/finland-news/domestic/8331-paatero-police-wants-authority-to-monitor-internet-traffic.html / 3.7.2014]

Iltalehti 26.1.2013, *Kasvi lyttää: Kyberturvallisuusstrategia on vitsi*. [http://www.iltalehti.fi/uutiset/2013012616603425_uu.shtml / 4.7.2014]

Kaleva 12.1.2015, *Kiuru verkkovalvontamietinnössä: Kuin sallisi kotietsinnän joka kotiin*. [http://www.kaleva.fi/uutiset/kotimaa/kiuru-verkkovalvontamietinnosta-kuin-sallisi-kotietsinnan-joka-kotiin/686451/ / 12.1.2015]

MTV-uutiset 31.10.2013, *Suomen ulkoministeriö laajan verkkovakoilun kohteena*. [http://www.mtv.fi/uutiset/kotimaa/artikkeli/mtv3--suomen-ulkoministerio-laajan-verkkovakoilun-kohteena-vuosia/2369718 / 15.4.2014]

Sveriges radio 3.11.2013, *Sverige avslöjade spionage i Finland*. [http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5693167 / 15.4.2014]

SvD nyheter 3.9.2014, *Säpo hindrade två terrordåd*. [www.svd.se/nyheter/inrikes/sapo-stoppade-terrordad_3877326.svd?sidan=1 / 5.3.2015]

Talouselämä 20.6.2013, *Supo haluaa seurata sinua tarkemmin verkossa*. [http://www.talouselama.fi/uutiset/supo+haluaa+seurata+sinua+tarkemmin+verkossa/a2191293 / 3.7.2014]

The Guardian 6.6.2013, *NSA collecting phone records of millions of Verizon customers daily*. [http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order / 18.7.2014]

YLE nyheter 18.11.2013, *Staten ska inte övervaka din Facebook*. [http://svenska.yle.fi/artikel/2013/11/08/staten-ska-inte-overvaka-din-facebook / 4.7.2014]

YLE nyheter 3.7.2014, *Viranomaisia ei kiinnosta, mitä Facebookissasi tapahtuu*. [http://yle.fi/uutiset/haglund_viranomaisia_ei_kiinnosta_mita_facebookissasi_tapahtuu/7336651 / 4.7.2014]

YLE nyheter 29.11.2014, *Supo: Suomessa yhtä paljon vakoojia kuin kylmän sodan aikana.* [http://yle.fi/uutiset/supo_suomessa_yhta_paljon_vakoojia_kuin_kylman_sodan_aikana/7659743 / 5.3.2015]

YLE nyheter 14.1.2015, *Försvarsmakten och Skypo föreslås få spana på nätet.* [http://svenska.yle.fi/artikel/2015/01/14/forsvarsmakten-och-skypo-foreslas-fa-spana-pa-natet / 5.3.2015]

YLE tv-nyheter, TV2 kl. 21.50, 2.7.2014.

Forskningslitteratur och -artiklar

Bigo, Didier. "International Political Sociology", Williams, Paul D. (ed), *Security Studies – An Intorduction*, 1st ed., Routledge, Abingdon 2008.

Buzan, Barry & Wæver, Ole & de Wilde, Jaap. *Security: A New Framework for Analysis*, Lynne Rienner Publishers, London 1998.

Deibert, Ronald. "Divide and Rule: Republican Security Theory as Civil Society Cyber Strategy", Famularo, Julia M. & Kepe, Marta. (ed.), *International Engagement on Cyber III: State Building on a New Frontier*, Georgetown Journal of International Affairs, Institute for Law, Science & Global Security, Washington 2013.

Emmers, Ralf. "Securitization", Collins, Alan. (ed), *Contemporary Security Studies*, 2nd ed., Oxford University Press, Oxford 2010.

Kamal, Ahmad. *The Law of Cyber-Space: an invitation to the table of negotiations*, United Nations, Institute of Training and Research, New York 2005.

Kiravuo, Timo. "Offensive Cyber-capabilities against Critical Infrastructure", Vankka, Jouko. (ed). *Cyber Warfare*, National Defence University, Department of Military Technology, Publication Series 1, No. 34, Helsingfors 2013.

Limnéll, Jarno. *Suomen uhkakuvapolitiikka 2000-luvun alussa*, Maanpuolustuskorkeakoulu, Strategian Laitos, julkaisusarja 1, Strategian tutkimuksia No. 29, Helsingfors 2009.

Luoma, Pentti. *Johdatus kvalitatiiviseen vertailevaan analyysiin*, Oulun yliopisto 23.11.2006. [www.oulu.fi/sosiologia/node/5047 / 30.1.2015]

OECD, "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, 2012. [http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf / 1.3.2014]

Ragin, Charles C. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*, University of California Press Ltd, London 1989.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations", Vankka, Jouko. (ed). *Cyber Warfare*, National Defence University, Department of Military Technology, Publication Series 1, No. 34, Helsingfors 2013.

Sipilä, Joonas & Koivula, Tommi. *Kuinka strategiaa tutkitaan*, Maanpuolustuskorkeakoulu, Strategian laitos, julkaisusarja 2, Tutkimusselosteita No. 50, Helsingfors 2013.

Tikk-Ringas, Eneken. "Cyber Security: Solutions of Tomorrow, Experience of Yesterday", Huldt, Bo & Sivonen, Pekka & Ries, Tomas & Huldt, Camilla. (ed) *Strategic Yearbook 2012-2013. The Emerging Global Security Environment*, Edita Västra Aros, Västerås 2013.

Zakheim, Dov S. "The Opportunity Cost of Security", *Prism*, Vol. 3, No.3, 2014. [http://cco.dodlive.mil/files/2014/02/prism119-124_zakheim.pdf / 1.3.2014]

BILAGOR

BILAGA 1. EN SAMMANFATTNING AV JÄMFÖRELSEN MELLAN FINLANDS OCH SVERIGES CYBERSÄKERHETSPOLITIK.

ANALYSERAT OMRÅDE	LIKA/OLIKA	FINLAND	SVERIGE
Syn på cybersäkerhetspolitik	Lika	Sättet att behandla cybersäkerheten som en del av den övriga säkerhetspoltiken och det så kallade totalförsvarstänkandet.	
Syn på ansvarsuppdelning myndigheterna emellan	Lika	Syn på polisens roll som ledande myndighet av övervakningen och utredande av brott i cyberrymden.	
Säkerhetiseringsmetod	Olika	Den nationella cybersäkerhetsstrategin stödda av övriga statliga dokument.	Statliga dokument som behandlar informationssäkerhet.
Styrkor i den utförda cybersäkerhetspolitiken	Olika	Ett målmedvetet strategiskt arbete för att få kontroll över cyberdomänet.	Förmågan att fatta strategiskt betydande beslut i form av FRA-lagen samt det tidiga uppbyggandet av en fungerande säkerhetsstruktur.
Svagheter i den utförda cybersäkerhetspolitiken	Olika	Brist på en centraliserad ledning och uppmärksammande av näringslivets behov.	Avsaknad av entydig vision om hur myndigheternas sammarbete skall bindas samman.
Lagstiftning	Lika	Betonande av medborgarnas grundläggande rättigheter och friheter, yttrandefrihet samt integritet i cyberrymden.	
Lagstiftning	Lika	Betonande av den internationella lagstiftningsprocessens nödvändighet.	
Lagstiftning	Lika	Cyberterminologin måste definieras juridiskt.	
Lagstiftning	Olika	Avsikter att förnya lagstiftningen.	Avsikter att anpassa lagstiftningen.